

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2001 年 7 月 5 日 (05.07.2001)

PCT

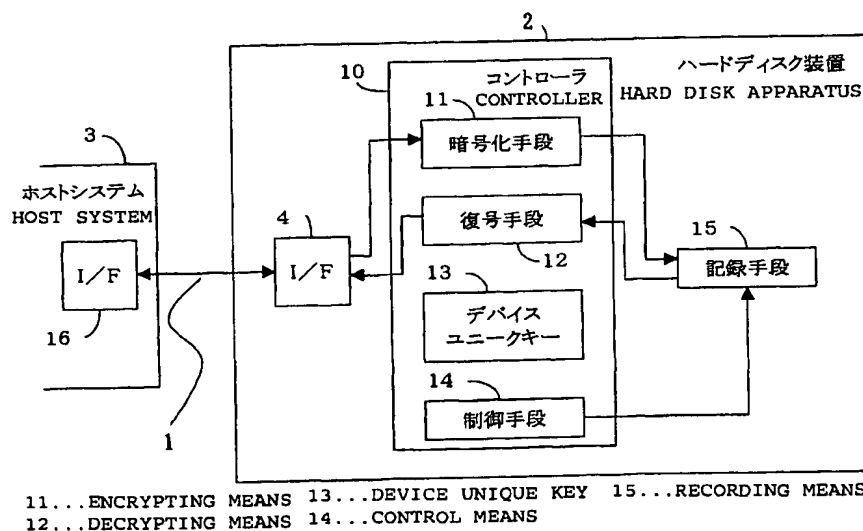
(10) 国際公開番号
WO 01/48755 A1

- (51) 国際特許分類: G11B 20/10, 20/12, G06F 17/60, 3/06, H04N 5/91, H04L 9/00
- (21) 国際出願番号: PCT/JP00/09260
- (22) 国際出願日: 2000 年 12 月 26 日 (26.12.2000)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願平 11/375777 1999 年 12 月 28 日 (28.12.1999) JP
特願2000/247688 2000 年 8 月 17 日 (17.08.2000) JP
- (71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府門真市大字門真 1006 番地 Osaka (JP).
- (72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 吉田修一 (YOSHIDA, Shuichi) [JP/JP]; 〒555-0024 大阪府大阪市西淀川区野里 2-7-25 Osaka (JP). 岡田孝文 (OKADA, Takanori) [JP/JP]; 〒560-0045 大阪府豊中市刀根山 6-5-76-102 Osaka (JP). 久野良樹 (KUNO, Yoshiki) [JP/JP]; 〒570-0054 大阪府守口市大枝西町 14-26-204 Osaka (JP). 米野潤一 (KOMENO, Jyun-ichi) [JP/JP]; 〒536-0001 大阪府大阪市城東区古市 3-1-2-1202 Osaka (JP). 神門俊和 (KOUDO, Toshikazu) [JP/JP]; 〒663-8102 兵庫県西宮市松並町 13-5-302 Hyogo (JP). 清水亮輔 (SHIMIZU, Ryosuke) [JP/JP]; 〒573-1111 大阪府枚方市楠葉朝日 3-10-31 Osaka (JP). 久保徳章 (KUBO, Noriaki) [JP/JP]; 〒560-0045 大阪府高槻市月見町 3-1-508 Osaka (JP).
- (74) 代理人: 弁理士 松田正道 (MATSUDA, Masamichi); 〒532-0003 大阪府大阪市淀川区宮原 5 丁目 1 番 3 号 新大阪生島ビル Osaka (JP).

[続葉有]

(54) Title: RECORDING APPARATUS, REPRODUCING APPARATUS, DATA PROCESSING APPARATUS, RECORDING/REPRODUCING APPARATUS, AND DATA TRANSMITTING APPARATUS

(54) 発明の名称: 記録装置、再生装置、データ処理装置、記録再生装置、データ送信装置



(57) Abstract: There has been conventionally no concrete contrivance to protect copyright when AV data is recorded in a recording apparatus and/or when data is reproduced by a reproducing apparatus. A recording apparatus comprising encrypting means (11) for encrypting AV data sent from an interface (4), control means (14) for control to record encrypted AV data, recording means (15) controlled by the control means (14) so as to record encrypted AV data on a magnetic disk, wherein the control means (14) carries out control to reproduce recorded data, the recording means (15) is controlled by the control means (14) and reproduces data recorded on a disk, and decrypting means (12) decrypts the reproduced data and sends it to an interface.

[続葉有]

WO 01/48755 A1

WO 01/48755 A1



(81) 指定国 (国内): CN, JP, KR, SG, US.

2 文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

添付公開書類:

- 国際調査報告書
- 請求の範囲の補正の期限前の公開であり、補正書受領の際には再公開される。

(57) 要約:

AVなどのデータを記録装置に記録する場合及び／またはデータを再生装置で再生する場合に著作権を保護する具体的な仕組みがない。

インターフェース4から送られてくるAVデータを暗号化する暗号化手段11と、暗号化されたAVデータを記録するよう制御する制御手段14と、制御手段14によって制御され、暗号化されたAVデータを磁気ディスクに記録する記録手段15とを備え、制御手段14は、記録されたデータを再生するよう制御し、記録手段15は制御手段14によって制御され、ディスクに記録されたデータを再生し、復号手段12は、再生されたデータを復号してインターフェースに送る。

WO 01/48755

PCT/JP00/09260

1.

明 細 書

記録装置、再生装置、データ処理装置、記録再生装置、データ送信装置

技術分野

本発明は、データを記録する記録装置、データを再生する再生装置、記録媒体に記録されているデータを他の装置へ移動させるまたは複写するデータ処理装置、そのように移動してきたデータを記録し再生する記録再生装置、複数のデータで構成されているストリームを送信するデータ送信装置、テレビ放送等にて放送されるコンテンツを、所定の時間遅らせて視聴するタイムシフト再生を行うための記録装置と記録再生装置に関するものである。

背景技術

新作の映画や有料放送のテレビ番組、音楽などの著作権保護が必要なデータを扱う場合、著作権を保護することが必要である。著作権を保護するための有力な方法として、著作権を保護する必要があるデータを暗号化してデータの利用に制限を加える方法がある。

例えば、映像音声データ（以下AVデータと記す）を伝送する際、AVデータを著作権保護する必要がある場合、そのAVデータを暗号化して伝送することが行われている。そのような例としてIEEE1394-DTSP (Digital Transmission Protection) 方式が規格化されている。

WO 01/48755

PCT/JP00/09260

2

IEEE 1394は、シリアル伝送を行う高速バスシステムで、データを同期伝送できるため、AVデータなどのリアルタイム伝送が可能である。このようなIEEE 1394は、家庭用デジタルAV機器を始め、多くのデジタル映像音声機器に外部用インターフェースとして搭載されようとしている。

IEEE 1394-DTSP方式によれば、IEEE 1394バスでデータ伝送する際に、認証機能と鍵の無効化機能を備えており、AVデータなどの著作権保護が必要なデータを暗号化して伝送することにより著作権の保護を実現することが出来る。

さて、パーソナルコンピュータの普及と進歩に伴い、外部記憶装置としてその大容量性、高速性からハードディスク装置などの記録装置や再生装置が数多く用いられている。さらに、最近ハードディスク装置は、コンピュータのみならず、デジタル技術を応用して映像、音声を記録再生するデジタルAV機器などにもその高速性、大容量性を生かして用いられつつある。

このように従来から映画の創作者等は、自ら作成したデータを第三者に勝手にコピーさせたくないと考える場合がある。そこで、著作権を保護するために、他の記録媒体へのコピーをすることが禁止されているデータや、1回のみのコピーだけが許されているデータというものが存在する。

そのようなデータは、例えばHDDにコピーして蓄積された場合であれば、そのHDDにおいてのみ再生されるということになる。

また、テレビ放送の視聴法の1つとして、放送された番組（コンテンツ）を一時的にVTR等の記録装置に記録しておき、記録したデータを後に再生することにより、本来の放送時刻と異なる時刻に番組を視聴することは従来より盛んに行われている。

特に、記録装置に、ハードディスク等の、ランダムアクセス可能であり、記録再生が同時に可能な記録媒体を用いた場合は、従来のテープ媒体を用いたVTRに対し、番組の放送時間内であるわずかな時間だけ遅れた後にでも、当該番組の内容を欠かすことなく連続して視聴することができるなどの、狭義のタイムシフト再生を実現することができる。

図43は、従来の技術による、タイムシフト再生を実現するための記録再生装置の構成図である。図に示すように、記録再生手段2120は、外部からの放送を記録再生するための手段、記録媒体2130は、ハードディスク等で実現される、放送のデータを蓄積するための手段、切り替え手段2160は、記録再生手段2120からの入力と、外部からの放送の入力とを受け、いずれかを選択して外部のモニタ等へ出力する手段である。

このような構成を有する従来の技術による記録再生装置の動作の一例を以下に説明する。

はじめに、視聴者が、リアルタイムで番組を視聴している場合、切り替え手段2160は、外部からの放送をそのままモニタへ出力するよう設定する一方で、記録再生手段2120は、同一の番組内容を記録媒体2130へ記録している。

次に、視聴者が、一時的にモニタの前を離れた後、再びモニタの前に戻り、番組の視聴を再開する場合は、記録再生手段2120は、視聴者がモニタの前を離れた時点から、記録したデータを再生し、切り替え手段2160は記録再生手段2120からの入力をモニタへ出力するように設定する。これ以後、視聴者は、番組として、記録再生手段2120からの再生出力を視聴することになる。

WO 01/48755

PCT/JP00/09260

4

上記の動作において、記録再生手段 2 1 2 0 は、データを再生する一方で、外部からの放送の録画も平行して行う。すなわち、記録再生手段 2 1 2 0 は、データの再生と記録を同時に行っている。

これにより、視聴者は、リアルタイムで放送されている番組を視聴する際に、一時的に視聴を中断しなければならないような場合でも、視聴の中断時間だけ遅れて、番組の内容を切れ目無く把握しつつ視聴することが可能となる。

ところが、AVデータを伝送する場合と同様に、著作権保護を必要とするAVデータをハードディスク装置などの記録媒体に記録する場合及び／または再生する場合にも著作権を保護する仕組みが必要である。ところが、記録装置及び／または再生装置に著作権保護を必要とするAVデータを記録及び／または再生する場合にどのようにして著作権を保護するかは具体的に決定されていない。

また、AVデータに限らず、インターネットなどから送られてくる文書データや、ゲームソフトなどのコンピュータプログラムについてもAVデータと同様に著作権保護を必要とする場合がある。しかしながら、記録装置及び／または再生装置に著作権保護を必要とするこのようなデータを記録及び／または再生する場合にどのようにして著作権を保護するかは具体的に決定されていない。

すなわち、AVデータや文書データやコンピュータプログラムなどのデータを記録装置に記録する場合及び／またはこれらのデータを再生装置で再生する場合に著作権を保護する具体的な仕組みがないという課題がある。

また、上記のHDDのデータ記録残存容量が少なくなってくると、HDDに記録されているデータの上に新たなデータを上書きしたり、HDDに記録されている一部のデータを削除して残存容量を増やす必要がでてくる。しか

WO 01/48755

PCT/JP00/09260

5

しながら、HDDのユーザは、HDDに記録されているデータへの上書きや、データの削除をしたくないと考え、HDDに記録されているデータを他の記録媒体にコピーしたいと考える場合がある。

他方、上述したように著作権者は、HDDに記録されたデータを著作権を無視してコピーされると困る。

すなわち、著作権保護が必要なデータをHDDなどの記録装置に記録している場合、ユーザは、そのデータを他の記録媒体にコピーすることが出来ないという課題がある。

また、ケーブルテレビやCS放送等の、放送形態の多様化、信号のデジタル化等により、放送される番組にも著作権上の問題が考慮され、信号にコピーガードを含むことにより、複製のための記録があらかじめ不可能に設定された番組の放映が実現されている。

しかしながら、従来の記録再生装置において、上述のような著作権を考慮した番組に対してタイムシフト再生を実現するためには、記録媒体2130に番組を記録することが、番組に関する著作権の侵害を引き起こす恐れがあるという問題があった。

すなわち、著作権保護が必要な番組についてタイムシフト再生を実現すると、番組に関する著作権の侵害を引き起こす恐れがあるという課題がある。

このような問題を回避する方策としては、(1)タイムシフトが可能な時間を制限する。(2)放送されるコンテンツが丸ごと保存されることを防ぐ等の方法が考えられる。

WO 01/48755

PCT/JP00/09260

6

発明の開示

本発明は、上記課題を考慮し、著作権保護が必要なデータを記録する場合及び／または著作権保護が必要なデータを再生する場合に著作権を保護することが出来る記録装置及び再生装置を提供することを目的とするものである。

また、本発明は、上記課題を考慮し、著作権を保護しつつ、コピーが禁止されているデータを他の記録媒体に移動させるまたは複写するデータ処理装置と、そのデータ処理装置からのデータを記録媒体に記録し、または記録するとともに再生する記録再生装置と、著作権を保護してデータをバックアップしておく暗号化データ復号記録装置システムおよびそのシステムを構成する復号記録装置、記録装置と、著作権を保護してデータを送信するデータ送信装置とを提供することを目的とするものである。

また、本発明は、上記課題を考慮し、本来の放送時間より遅れて視聴を行うためのタイムシフト再生において、著作権侵害を回避することが可能な、記録装置、及び記録再生装置を提供することを目的とするものである。

上述した課題を解決するために、第1の発明（請求項1に対応）は、インターフェースから送られてくるデータを暗号化する暗号化手段と、

前記暗号化されたデータを記録するよう制御する制御手段と、

前記制御手段によって制御され、前記暗号化されたデータをディスクに記録する記録手段とを備えたことを特徴とする記録装置である。

また、第2の発明（請求項2に対応）は、前記暗号化手段は、記録装置自らに割り付けられた固有の数値及び／または記号であるデバイスユニークキーを用いて、前記データを暗号化することを特徴とする第1の発明に記載の記録装置であ

WO 01/48755

PCT/JP00/09260

7

る。

また、第3の発明（請求項3に対応）は、前記暗号化手段は、前記制御手段が前記記録手段に連続してアクセスする最小単位である記録ユニットに対応する記録ブロックに固有の番号及び／または記号である記録ユニット情報を用いて、前記データを暗号化することを特徴とする第1または2の発明に記載の記録装置である。

また、第4の発明（請求項4に対応）は、前記記録ユニット情報を用いて、前記データを暗号化することは、前記記録ユニット情報に基づいて得られたキーで前記データを暗号化することであることを特徴とする第3の発明に記載の記録装置である。

また、第5の発明（請求項5に対応）は、少なくとも前記記録ブロックに記録される前記暗号化されたデータ及び前記暗号化されたデータに付加された付加情報は、すべての部分が暗号化されて前記記録手段に記録されることを特徴とする第3または4の発明に記載の記録装置である。

また、第6の発明（請求項6に対応）は、前記データには、コピー許諾情報が付加されており、

前記制御手段は、前記コピー許諾情報を前記記録手段が記録するように前記記録手段を制御し、

前記暗号化手段は、前記デバイスユニークキーと前記コピー許諾情報の少なくともいずれかを含む第1の情報を作成し、

前記記録ユニット情報を用いて、前記暗号化手段は、前記第1の情報を暗号化した情報であるコンテンツキーを生成し、

前記暗号化手段は、前記コンテンツキーを用いて前記データを暗号化し、

WO 01/48755

PCT/JP00/09260

前記制御手段は前記暗号化したデータを前記記録手段が記録するように前記記録手段を制御することを特徴とする第3～5の発明のいずれかに記載の記録装置である。

また、第7の発明（請求項7に対応）は、前記データには、前記データに固有の数値及び／または記号であるタイトルキーが割り付けられており、

前記暗号化手段は、前記タイトルキーを前記デバイスユニークキーを用いて暗号化し、

前記制御手段は、前記暗号化されたタイトルキーを前記記録手段に記録するように前記記録手段を制御することを特徴とする請求項2記載の記録装置。

また、第8の発明（請求項8に対応）は、前記暗号化手段は、前記タイトルキーを用いて前記データを暗号化することを特徴とする第7の発明に記載の記録装置である。

また、第9の発明（請求項9に対応）は、前記暗号化手段は、前記タイトルキーを前記デバイスユニークキーを用いて暗号化し、

前記制御手段は、前記暗号化されたタイトルキーを前記記録手段が記録するように前記記録手段を制御し、

前記暗号化手段は、前記タイトルキーを含む第3の情報を作成し、

前記制御手段が前記記録手段に連続してアクセスする最小単位である記録ユニットを前提とする記録ブロックに固有の番号及び／または記号である記録ユニット情報を用いて、前記暗号化手段は、前記第3の情報を暗号化した情報であるコンテンツキーを生成し、

前記暗号化手段は、前記コンテンツキーを用いて前記データを暗号化し、

前記制御手段は前記暗号化したデータを前記記録手段が記録するように前記記

WO 01/48755

PCT/JP00/09260

9

録手段を制御することを特徴とする第 8 の発明に記載の記録装置である。

また、第 10 の発明（請求項 10 に対応）は、前記データには、コピー許諾情報が付加されており、

前記暗号化手段は、前記コピー許諾情報をも用いて、前記データを暗号化することを特徴とする第 8 の発明に記載の記録装置である。

また、第 11 の発明（請求項 11 に対応）は、前記暗号化手段は、前記タイトルキーを前記デバイスユニークキーを用いて暗号化し、

前記制御手段は、前記暗号化されたタイトルキーを前記記録手段が記録するように前記記録手段を制御し、

前記制御手段は、前記コピー許諾情報を前記記録手段が記録するように前記記録手段を制御し、

前記暗号化手段は、前記タイトルキーと前記コピー許諾情報の少なくともいずれかを含む第 2 の情報を作成し、

前記制御手段が前記記録手段に連続してアクセスする最小単位である記録ユニットを前提とする記録ブロックに固有の番号及び／または記号である記録ユニット情報を用いて、前記暗号化手段は、前記第 2 の情報を暗号化した情報であるコンテンツキーを生成し、

前記暗号化手段は、前記コンテンツキーを用いて前記データを暗号化し、

前記制御手段は前記暗号化したデータを前記記録手段が記録するように前記記録手段を制御することを特徴とする第 10 の発明に記載の記録装置である。

また、第 12 の発明（請求項 12 に対応）は、前記暗号化手段は、コピー許諾情報が付加され、インターフェースから送られてくるデータを前記コピー許諾情報を用いて暗号化し、

WO 01/48755

PCT/JP00/09260

10

前記制御手段は、前記記録手段が前記データを記録する前及び／または前記データを記録した後に、前記コピー許諾情報を記録するよう前記記録手段を制御することを特徴とする第1の発明に記載の記録装置である。

また、第13の発明（請求項13に対応）は、前記制御手段は、少なくとも前記記録手段が前記データを記録する前に、前記コピー許諾情報を記録するよう前記記録手段を制御することを特徴とする第12の発明に記載の記録装置である。

また、第14の発明（請求項14に対応）は、前記制御手段は、前記記録手段が前記データを記録した後のみに、前記コピー許諾情報を記録するよう前記記録手段を制御することを特徴とする第12の発明に記載の記録装置である。

また、第15の発明（請求項15に対応）は、インターフェースから送られてくる暗号化されたデータを記録するよう制御する制御手段と、

前記制御手段によって制御され、前記暗号化されたデータをディスクに記録する記録手段とを備えたことを特徴とする記録装置である。

また、第16の発明（請求項16に対応）は、第1の発明に記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、
前記再生されたデータを復号してインターフェースに送る復号手段とを備えたことを特徴とする再生装置である。

また、第17の発明（請求項17に対応）は、第2の発明に記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

WO 01/48755

PCT/JP00/09260

11

前記再生されたデータを復号してインターフェースに送る復号手段とを備え、
前記復号手段は、前記デバイスユニークキーを用いて前記再生されたデータを復号することを特徴とする再生装置である。

また、第18の発明（請求項18に対応）は、第3の発明に記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、
前記再生されたデータを復号してインターフェースに送る復号手段とを備え、
前記復号手段は、前記記録ユニット情報を用いて前記再生されたデータを復号することを特徴とする再生装置である。

また、第19の発明（請求項19に対応）は、第4の発明に記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、
前記再生されたデータを復号してインターフェースに送る復号手段とを備え、
前記復号手段は、前記記録ユニット情報に基づいて得られたキーで前記再生されたデータを復号することを特徴とする再生装置である。

また、第20の発明（請求項20に対応）は、第14の発明に記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、
前記再生されたデータを復号してインターフェースに送る復号手段とを備え、
前記データの記録時に、前記コピー許諾情報が前記記録手段に正常に記録出来

WO 01/48755

PCT/JP00/09260

12

なかった場合、前記復号手段は、前記コピー許諾情報が各値を取ると仮定して前記暗号化されたデータの全部または一部の復号を試行し、

前記試行した結果、前記再生されたデータが正常に復号出来た場合の前記コピー許諾情報の値を用いて前記再生されたデータを復号することを特徴とする再生装置である。

また、第 2 1 の発明（請求項 2 1 に対応）は、第 1 5 の発明に記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段とを備え、

前記再生されたデータは、インターフェースに送られることを特徴とする再生装置。

また、第 2 2 の発明（請求項 2 2 に対応）は、前記インターフェース、前記暗号化手段及び前記制御手段が、同一プリント基板上に一体化して配設されていることを特徴とする第 1 ～ 1 4 の発明のいずれかに記載の記録装置である。

また、第 2 3 の発明（請求項 2 3 に対応）は、前記インターフェース、前記暗号化手段及び前記制御手段は、1 チップ化されていることを特徴とする第 2 2 の発明に記載の記録装置である。

また、第 2 4 の発明（請求項 2 4 に対応）は、前記インターフェース、前記復号手段及び前記制御手段が同一プリント基板上に一体化して配設されていることを特徴とする第 1 6 ～ 2 0 の発明のいずれかに記載の再生装置である。

また、第 2 5 の発明（請求項 2 5 に対応）は、前記インターフェース、前記復号手段及び前記制御手段は、1 チップ化されていることを特徴とする第 2 4 の発明に記載の再生装置である。

WO 01/48755

PCT/JP00/09260

13

また、第 26 の発明（請求項 26 に対応）は、データとして再生出来る信号を出力している、前記プリント基板上の端子から検出される信号は、全て暗号化されているか及び／または非公開のフォーマットで記述されていることを特徴とする第 22 の発明に記載の記録装置である。

また、第 27 の発明（請求項 27 に対応）は、第 3 者がデータとして再生出来る信号を出力している、前記プリント基板上の端子から検出される信号は、全て暗号化されているか及び／または非公開のフォーマットで記述されていることを特徴とする第 24 の発明に記載の再生装置である。

また、第 28 の発明（請求項 28 に対応）は、第 3 者がデータとして再生出来る信号を出力している、前記プリント基板上の端子の性質は、非公開のフォーマットで定められていることを特徴とする第 22 の発明に記載の記録装置である。

また、第 29 の発明（請求項 29 に対応）は、第 3 者がデータとして再生出来る信号を出力している、前記プリント基板上の端子の性質は、非公開のフォーマットで定められていることを特徴とする第 24 の発明に記載の再生装置である。

また、第 30 の発明（請求項 30 に対応）は、前記デバイスユニークキーは、外部の機器がアクセスすることが出来ないことを特徴とする第 2～11 の発明のいずれかに記載の記録装置である。

また、第 31 の発明（請求項 31 に対応）は、前記コピー許諾情報は、前記記録手段のユーザから直接アクセスできないシステム領域に記録されることを特徴とする第 6、10、11、12、13、14 の発明のいずれかに記載の記録装置である。

また、第 32 の発明（請求項 32 に対応）は、前記インターフェースから送られてくるデータには、コピー許諾情報が付加されており、

WO 01/48755

PCT/JP00/09260

14

前記制御手段は、所定の条件のもとで、前記データの前記コピー許諾情報が、複製禁止 (copy never) を表す場合であっても、前記記録手段が前記データを記録するように制御することが出来ることを特徴とする第1～15、22、23、26、28、30、31の発明のいずれかに記載の記録装置である。

また、第33の発明 (請求項33に対応) は、前記所定の条件とは、記録された前記データが所定の時間後に再生不可となる場合であることを特徴とする第32の発明に記載の記録装置である。

また、第34の発明 (請求項34に対応) は、前記所定の条件とは、記録された前記データが課金条件によって再生不可となる場合であることを特徴とする第32の発明に記載の記録装置である。

また、第35の本発明 (請求項35に対応) は、前記記録された暗号化されたデータには、コピー許諾情報が付加されており、

前記制御手段は、所定の条件のもとで、前記データの前記コピー許諾情報が、複製禁止 (copy never) を表す場合、前記再生手段が前記データを少なくとも1回再生するよう制御することを特徴とする第16～21、24、25、27、29の本発明のいずれかに記載の再生装置である。

また、第36の発明 (請求項36に対応) は、前記所定の条件とは、記録された前記データが所定の時間後に再生不可となる場合であることを特徴とする第35の発明に記載の再生装置である。

また、第37の発明 (請求項37に対応) は、前記所定の条件とは、記録された前記データが課金条件によって再生不可となる場合であることを特徴とする第35の発明に記載の再生装置である。

また、第38の発明 (請求項38に対応) は、前記記録された暗号化されたデ

WO 01/48755

PCT/JP00/09260

15

ータには、コピー許諾情報が付加されており、

前記制御手段は、所定の条件のもとで、前記データの前記コピー許諾情報が、1回だけ複製することを許可（copy once）することを表す場合、前記記録手段により1回複製された後の前記データの前記コピー許諾情報が、再び1回だけ複製することを許可（copy once）することを表すようにして、前記再生手段が前記データを1回だけ複製出力するよう制御することを特徴とする第16～21、24、25、27、29の発明のいずれかに記載の再生装置である。

また、第39の発明（請求項39に対応）は、前記所定の条件とは、前記再生手段が前記データを複製出力した所定の時間後に、前記データもしくは前記データの暗号化に用いたキーを消去する場合であることを特徴とする第38の発明に記載の再生装置である。

また、第40の発明（請求項40に対応）は、前記所定の条件とは、1回だけ複製出力された前記データの記録先がバックアップ用として前記データを記録する装置である場合であることを特徴とする第38の発明に記載の再生装置である。

また、第41の発明（請求項41に対応）は、前記記録先でバックアップ用として記録された前記データは、前記記録先では再生不可であることを特徴とする第40の発明に記載の再生装置である。

また、第42の発明（請求項42に対応）は、前記記録先でバックアップ用として記録された前記データは、元の再生装置に戻さない限り再生不可であることを特徴とする第40の発明に記載の再生装置である。

また、第43の発明（請求項43に対応）は、前記暗号化手段は、前記インターフェースから送られてくるデータのコピー許諾情報の値に関係なく前記データ

WO 01/48755

PCT/JP00/09260

16

を暗号化することを特徴とする第1～14、22、23、26、30～34の初
s めいのいずれかに記載の記録装置である。

また、第44の発明（請求項44に対応）は、前記暗号化手段は、前記インターフェースから送られてくるデータのコピー許諾情報が自由に複製してもよいこと（Copy free）を表す場合、前記データを暗号化せず、

前記制御手段は、前記記録手段が前記暗号化されていないデータを記録するように制御することを特徴とする第1～14、22、23、26、30～34の発明のいずれかに記載の記録装置である。

また、第45の発明（請求項45に対応）は、データが記録される記録媒体に記録されているデータを他の記録装置へ移動させる移動手段を少なくとも備えたデータ処理装置であって、

前記移動手段が移動させようとするデータがコピーが禁止されているコピー禁止データである場合、そのコピー禁止データは、少なくとも前記データ処理装置から出力するときには、前記データ処理装置固有の暗号化鍵で暗号化されている

ことを特徴とするデータ処理装置である。

また、第46の発明（請求項46に対応）は、データが記録される記録媒体に記録されているデータを他の記録装置に複写する複写手段を少なくとも備えたデータ処理装置であって、

前記複写手段が複写しようとするデータがコピーが禁止されているコピー禁止データである場合、そのコピー禁止データは、少なくとも前記データ処理装置から出力するときには、前記データ処理装置固有の暗号化鍵で暗号化されている

WO 01/48755

PCT/JP00/09260

17

ことを特徴とするデータ処理装置である。

また、第４７の発明（請求項４７に対応）は、前記コピー禁止データを前記暗号化鍵で暗号化する暗号化手段をさらに備えたことを特徴とする第４５または４６の発明に記載のデータ処理装置である。

また、第４８の発明（請求項４８に対応）は、前記暗号化鍵で暗号化されている前記コピー禁止データを、前記暗号化鍵を用いて解読し、前記コピー禁止データを再生する再生手段をさらに備えたことを特徴とする第４５～４７の発明のいずれかに記載のデータ処理装置である。

また、第４９の発明（請求項４９に対応）は、前記再生手段は、ユーザが視聴するさいに必要な速度で前記コピー禁止データを再生する手段であって

前記他の記録装置から前記ユーザが視聴するさいに必要な速度よりも速い速度で、前記暗号化鍵で暗号化されている前記コピー禁止データが送信されてきた場合、送信されてきた前記コピー禁止データを、前記ユーザが視聴するさいに必要な速度よりも速い速度で格納する格納手段をさらに備え、

前記再生手段は、前記格納手段が前記他の記録装置からの前記コピー禁止データを格納するさいに、前記格納手段に格納された前記コピー禁止データもしくは、予め前記格納手段に格納されたデータを再生することができる

ことを特徴とする第４８の発明に記載のデータ処理装置である。

また、第５０の発明（請求項５０に対応）は、前記他の記録装置が、第２の記録媒体へデータを記録することができる装置であって、

前記第２の記録媒体が前記データ処理装置に対応する記録媒体であるか否かを判断する判断手段をさらに備え、

WO 01/48755

PCT/JP00/09260

18

前記移動手段または前記複写手段は、前記判断手段によって、前記第 2 の記録媒体が前記データ処理装置に対応する記録媒体であると判断された場合、前記コピー禁止データを移動させるまたは複写する

ことを特徴とする第 45～49 の発明のいずれかに記載のデータ処理装置である。

また、第 51 の発明（請求項 51 に対応）は、前記他の記録装置が、第 2 の記録媒体へデータを記録することができる装置であって、

前記他の記録装置が前記データ処理装置に対応する装置であるか否かを判断する判断手段をさらに備え、

前記移動手段または前記複写手段は、前記判断手段によって、前記他の記録装置が前記データ処理装置に対応する装置であると判断された場合、前記コピー禁止データを移動させるまたは複写する

ことを特徴とする第 45～49 の発明のいずれかに記載のデータ処理装置である。

また、第 52 の発明（請求項 52 に対応）は、前記移動手段または前記複写手段は、前記コピー禁止データを移動させるまたは複写するさい、そのコピー禁止データを 1 回だけコピー可能なデータとして出力することを特徴とする第 45～51 の発明のいずれかに記載のデータ処理装置である。

また、第 53 の発明（請求項 53 に対応）は、第 45～47 の発明のいずれかに記載のデータ処理装置からの前記暗号化鍵で暗号化されている前記コピー禁止データを、第 2 の記録媒体に記録する記録手段を備えたことを特徴とする記録再生装置である。

また、第 54 の発明（請求項 54 に対応）は、第 48 の発明に記載のデー

WO 01/48755

PCT/JP00/09260

19

タ処理装置からの前記暗号化鍵で暗号化されている前記コピー禁止データを、第2の記録媒体に記録する記録手段と、

前記第2の記録媒体に記録された、前記暗号化鍵で暗号化されている前記コピー禁止データを、前記暗号化鍵で暗号化されているまま前記データ処理装置に送信する送信手段とを備えた

ことを特徴とする記録再生装置である。

また、第55の発明（請求項55に対応）は、第50または51の発明に記載のデータ処理装置からの前記暗号化鍵で暗号化されている前記コピー禁止データを、前記第2の記録媒体に記録する記録手段と、

前記第2の記録媒体に記録された、前記暗号化鍵で暗号化されている前記コピー禁止データを、前記暗号化鍵で暗号化されているまま前記データ処理装置に送信する送信手段とを備えた

ことを特徴とする記録再生装置である。

また、第56の発明（請求項56に対応）は、第45、46、47、50、51の発明のいずれかに記載のデータ処理装置からの前記暗号化鍵で暗号化されている前記コピー禁止データを、第2の記録媒体に記録する記録手段と、

前記第2の記録媒体に記録された、前記暗号化鍵で暗号化されている前記コピー禁止データを、前記暗号化鍵を用いて解読し、前記コピー禁止データを再生する解読再生手段とを備えた

ことを特徴とする記録再生装置である。

また、第57の発明（請求項57に対応）は、前記暗号化鍵が記録されている暗号化鍵記録媒体を再生する鍵再生手段と、

WO 01/48755

PCT/JP00/09260

20

前記鍵再生手段が再生した前記暗号化鍵を記憶する鍵記憶手段とをさらに備え、

前記解読再生手段は、前記鍵記憶手段が記憶している前記暗号化鍵を利用して、前記コピー禁止データを再生する

ことを特徴とする第 56 の発明に記載の記録再生装置である。

また、第 58 の発明（請求項 58 に対応）は、前記データ処理装置から送信されてきた前記暗号化鍵を受信する受信手段をさらに備え、

前記解読再生手段は、前記受信手段によって受信された前記暗号化鍵を利用して、前記コピー禁止データを再生する

ことを特徴とする第 56 の発明に記載の記録再生装置である。

また、第 59 の発明（請求項 59 に対応）は、データが記録される記録媒体に記録されているデータを、他の記録装置へ、その他の記録装置において解読される形式のデータとして移動させる移動手段を少なくとも備え、

前記移動手段が移動させようとするデータがコピーが禁止されているコピー禁止データである

ことを特徴とするデータ処理装置である。

また、第 60 の発明（請求項 60 に対応）は、データが記録される記録媒体に記録されているデータを、他の記録装置に、その他の記録装置において解読される形式のデータとして複写する複写手段を少なくとも備え、

前記複写手段が複写しようとするデータがコピーが禁止されているコピー禁止データである

ことを特徴とするデータ処理装置である。

また、第 61 の発明（請求項 61 に対応）は、前記他の記録装置において

WO 01/48755

PCT/JP00/09260

21

解読される形式のデータとは、平文データ、または前記他の記録装置固有の鍵で暗号化されたデータ、または前記他の記録装置における第2の記録媒体に付されている鍵で暗号化されたデータを意味することを特徴とする第59または60の発明に記載のデータ処理装置である。

また、第62の発明（請求項62に対応）は、前記他の記録装置において解読される形式のデータが、さらに、前記他の記録装置において用いられるフォーマットのデータでもあることを特徴とする第61の発明に記載のデータ処理装置である。

また、第63の発明（請求項63に対応）は、前記他の記録装置が、第2の記録媒体へデータを記録することができる装置であって、

前記第2の記録媒体が前記データ処理装置に対応する記録媒体であるか否かを判断する判断手段をさらに備え、

前記移動手段または前記複写手段は、前記判断手段によって、前記第2の記録媒体が前記データ処理装置に対応する記録媒体であると判断された場合、前記コピー禁止データを移動させるまたは複写する

ことを特徴とする第59～62の発明のいずれかに記載のデータ処理装置である。

また、第64の発明（請求項64に対応）は、前記第2の記録媒体に、前記第2の記録媒体が前記データ処理装置に対応する記録媒体であることを示す鍵が付されている場合、前記判断手段は前記鍵を用いて前記判断を行い、

前記判断手段によって、前記第2の記録媒体が前記データ処理装置に対応する記録媒体であると判断された場合、前記コピー禁止データを前記鍵を用いて暗号化する暗号化手段をさらに備え、

WO 01/48755

PCT/JP00/09260

22

前記移動手段または前記複写手段は、前記暗号化された前記コピー禁止データを移動させるまたは複写する

ことを特徴とする第63の発明に記載のデータ処理装置である。

また、第65の発明（請求項65に対応）は、前記他の記録装置が、第2の記録媒体へデータを記録することができる装置であって、

前記他の記録装置が前記データ処理装置に対応する装置であるか否かを判断する判断手段をさらに備え、

前記移動手段または前記複写手段は、前記判断手段によって、前記他の記録装置が前記データ処理装置に対応する装置であると判断された場合、前記コピー禁止データを移動させるまたは複写する

ことを特徴とする第59～62の発明のいずれかに記載のデータ処理装置である。

また、第66の発明（請求項66に対応）は、前記他の記録装置が、前記データ処理装置に対応する装置であることを示す鍵を有している場合、前記判断手段は前記鍵を用いて前記判断を行い、

前記判断手段によって、前記他の記録装置が前記データ処理装置に対応する装置であると判断された場合、前記コピー禁止データを前記鍵を用いて暗号化する暗号化手段をさらに備え、

前記移動手段または前記複写手段は、前記暗号化された前記コピー禁止データを移動させるまたは複写する

ことを特徴とする第65の発明に記載のデータ処理装置である。

また、第67の発明（請求項67に対応）は、前記移動手段または前記複写手段は、前記コピー禁止データを移動させるまたは複写するさい、そのコ

WO 01/48755

PCT/JP00/09260

23

ピー禁止データを1回だけコピー可能なデータとして出力することを特徴とする第59～66の発明のいずれかに記載のデータ処理装置である。

また、第68の発明（請求項68に対応）は、第59または60の発明に記載のデータ処理装置からの前記コピー禁止データを第2の記録媒体に記録し、再生する記録再生装置であって、

前記コピー禁止データが平文データであり、

前記コピー禁止データを、前記第2の記録媒体に付されている暗号化鍵を用いて、または前記記録再生装置固有の暗号化鍵を用いて暗号化する暗号化手段と、

前記暗号化手段によって暗号化された前記コピー禁止データを前記第2の記録媒体に記録する記録手段と、

前記第2の記録媒体に記録された、前記暗号化された前記コピー禁止データを、前記鍵を利用して解読し、再生する再生手段とを備えた

ことを特徴とする記録再生装置である。

また、第69の発明（請求項69に対応）は、第59または60の発明に記載のデータ処理装置からの前記コピー禁止データを第2の記録媒体に記録し、再生する記録再生装置であって、

前記コピー禁止データが前記記録再生装置固有の鍵で暗号化されたデータ、または前記第2の記録媒体に付されている鍵で暗号化されたデータであり、

前記暗号化された前記コピー禁止データを前記第2の記録媒体に記録する記録手段と、

前記第2の記録媒体に記録された、前記暗号化された前記コピー禁止デー

WO 01/48755

PCT/JP00/09260

24

タを、前記鍵を利用して解読し、再生する再生手段とを備えた

ことを特徴とする記録再生装置である。

また、第70の発明（請求項70に対応）は、前記移動手段が前記データの移動を行ったさい、または前記複写手段が前記データの複写を行ったさい、前記データの移動または複写に対する課金情報を、前記データ処理装置を管理する管理装置に送信する課金情報送信手段をさらに備えたことを特徴とする第45、46、47、48、49、50、51、52、59、60、61、62、63、64、65、66、67の発明のいずれかに記載のデータ処理装置である。

また、第71の発明（請求項71に対応）は、前記データ処理装置と前記他の記録装置とが接続されたインタフェースに、少なくとも前記コピー禁止データの移動または複写に対して課金能力を有する管理装置が接続されていることが確認されたときに、前記移動手段または前記複写手段は、前記コピー禁止データを前記他の記録装置に移動させるまたは複写することを特徴とする第45、46、47、48、49、50、51、52、59、60、61、62、63、64、65、66、67の発明のいずれかに記載のデータ処理装置である。

また、第72の発明（請求項72に対応）は、同じ内容の、コピーが禁止されているコピー禁止データが暗号化されてそれぞれ記録されている複数の記録装置と、

それら複数の記録装置から出力される前記暗号化された前記コピー禁止データを復号する復号手段と、前記コピー禁止データと同じ内容であって、暗号化され、または暗号化されていないコピー禁止データを記録する記録手段

WO 01/48755

PCT/JP00/09260

25

とを有する復号記録装置とを備えた

ことを特徴とする暗号化データ復号記録装置システムである。

また、第 7 3 の発明（請求項 7 3 に対応）は、同じ内容の、コピーが禁止されているコピー禁止データが暗号化されてそれぞれ記録されている複数の記録装置から出力される前記暗号化された前記コピー禁止データを復号する復号手段と、

前記コピー禁止データと同じ内容であって、暗号化され、または暗号化されていないコピー禁止データを記録する記録手段とを備えた

ことを特徴とする復号記録装置である。

また、第 7 4 の発明（請求項 7 4 に対応）は、同じ内容の、コピーが禁止されているコピー禁止データが暗号化されてそれぞれ記録されている複数の記録装置のうちの一つの記録装置であって、

前記暗号化された前記コピー禁止データを記録する記録手段と、その記録手段に記録されている前記暗号化されたコピー禁止データを出力する出力手段とを備え、

その出力手段から出力される前記暗号化されたコピー禁止データは、その暗号化されたコピー禁止データを復号する復号手段を少なくとも有する復号記録装置においてのみ復号されるデータである

ことを特徴とする記録装置である。

また、第 7 5 の発明（請求項 7 5 に対応）は、複数のデータで構成されているストリームを送信する送信手段を備え、

前記ストリームの、または前記ストリームを構成する各ブロック内の、複数の前記データそれぞれは、そのデータの時間上一つ手前のデータが再生

WO 01/48755

PCT/JP00/09260

26

されないと再生されないデータであって、

前記送信手段は、前記ストリームの、または前記ストリームを構成する各ブロック内の、前記複数個のデータの時間的に最後尾から先頭側の順に、前記各データを送信する

ことを特徴とするデータ送信装置である。

また、第76の発明（請求項76に対応）は、複製が禁止または制限されるよう設定されているデータからなる複製制限コンテンツをタイムシフト再生可能にするための記録装置であって、

所定の容量分、前記複製制限コンテンツの記録が可能な記録媒体と、

前記記録媒体に対しデータの記録を行う記録手段とを備え、

前記記録手段は、前記複製制限コンテンツを前記記録媒体に記録するとともに、前記複製制限コンテンツの記録を開始した時刻から、所定の時間が経過した後、前記記録媒体に記録された前記複製制限コンテンツのデータを、視聴することが不可能な状態にすることを特徴とする記録装置である。

また、第77の発明（請求項77に対応）は、前記視聴することが不可能な状態を、前記複製制限コンテンツのデータを消去することにより実現することを特徴とする第76の発明に記載の記録装置である。

また、第78の発明（請求項78に対応）は、前記視聴することが不可能な状態を、前記複製制限コンテンツのデータを消去しないことにより実現することを特徴とする第76の発明に記載の記録装置である。

また、第79の発明（請求項79に対応）は、前記視聴することが不可能な状態を、前記複製制限コンテンツのデータを再生不可能にすることにより実現することを特徴とする第76の発明に記載の記録装置である。

WO 01/48755

PCT/JP00/09260

27

また、第 80 の発明（請求項 80 に対応）は、前記視聴することが不可能な状態を、再生後の前記複製制限コンテンツのデータを暗号化することにより実現することを特徴とする第 79 の発明に記載の記録装置である。

また、第 81 の発明（請求項 81 に対応）は、前記記録手段が、前記複製制限コンテンツの記録を開始するタイミングは、前記複製制限コンテンツに関連した判別情報を参照することにより定められることを特徴とする第 76 ～ 80 の発明のいずれかに記載の記録装置である。

また、第 82 の発明（請求項 82 に対応）は、前記記録手段は、前記判別情報を用いて、前記複製制限コンテンツと他のコンテンツとを分別して記録を行うことを特徴とする第 81 の発明に記載の記録装置である。

また、第 83 の発明（請求項 83 に対応）は、前記判別情報は、前記複製制限コンテンツのデータ列に含まれる著作権情報であることを特徴とする第 81 の発明に記載の記録装置である。

また、第 84 の発明（請求項 84 に対応）は、前記記録手段が、前記複製制限コンテンツの記録を開始するタイミングは、外部からの入力に基づき定められることを特徴とする第 76 ～ 82 の発明のいずれかに記載の記録装置である。

また、第 85 の発明（請求項 85 に対応）は、前記記録媒体は、前記複製制限コンテンツの一時記録を行うための記録バッファを有することを特徴とする第 76 ～ 80 の発明のいずれかに記載の記録装置である。

また、第 86 の発明（請求項 86 に対応）は、前記記録用バッファは、同一領域に上書き記録を繰り返すことにより一定量のデータを記録することが可能なリングバッファであることを特徴とする第 85 の発明に記載の記録装

WO 01/48755

PCT/JP00/09260

28

置である。

また、第 87 の発明（請求項 87 に対応）は、第 76 ～ 85 の発明のいずれかに記載の記録装置と、

前記記録媒体に記録されたデータを再生する再生手段とを備えた記録再生装置であって、

前記再生手段は、前記複製制限コンテンツが記録開始された時刻から、所定の待機時間が経過した後、記録された前記複製制限コンテンツを再生することを特徴とする記録再生装置である。

また、第 88 の発明（請求項 88 に対応）は、第 86 の発明に記載の記録装置と、

前記記録媒体に記録されたデータを再生する再生手段とを備えた記録再生装置であって、

前記再生手段は、前記複製制限コンテンツが記録開始された時刻から、所定の待機時間が経過した後、記録された前記複製制限コンテンツを再生することを特徴とする記録再生装置である。

また、第 89 の発明（請求項 89 に対応）は、前記リングバッファに上書き記録が行われている状態で、前記再生手段が再生動作を行う際は、前記リングバッファ上にて、最も古いデータが記録されている位置から該データの再生を行うことを特徴とする第 88 の発明に記載の記録再生装置である。

また、第 90 の発明（請求項 90 に対応）は、前記リングバッファに上書き記録が行われていない状態で、前記再生手段が再生動作を行う際は、前記リングバッファ上の記録開始位置から前記データの再生を行うことを特徴とする第 89 の発明に記載の記録再生装置である。

WO 01/48755

PCT/JP00/09260

29

また、第 9 1 の発明（請求項 9 1 に対応）は、前記記録装置は、前記記録媒体に記録された複製制限コンテンツが、前記所定の待機時間内に再生されない場合、該複製制限コンテンツの記録動作を停止することを特徴とする第 8 7 または 8 8 の発明に記載の記録再生装置である。

また、第 9 2 の発明（請求項 9 2 に対応）は、前記所定の時間または前記所定の待機時間のいずれかに基づき、前記記録装置または再生手段の動作内容をあらかじめ告知する告知手段をさらに備えたことを特徴とする第 8 7 または 8 8 の発明に記載の記録再生装置である。

また、第 9 3 の発明（請求項 9 3 に対応）は、前記記録手段は、前記所定の時間を含む時間情報を、計測できることを特徴とする第 7 6 の発明に記載の記録装置である。

また、第 9 4 の発明（請求項 9 4 に対応）は、前記複製制限コンテンツは、前記所定の時間を含む時間情報を含んでいることを特徴とする第 7 6 の発明に記載の記録装置である。

また、第 9 5 の発明（請求項 9 5 に対応）は、前記所定の時間を含む時間情報を、前記複製制限コンテンツとは独立して外部から取得することを特徴とする第 7 6 の発明に記載の記録装置である。

また、第 9 6 の発明は、第 6 の発明に記載の記録装置によってディスク記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

前記再生されたデータを復号してインターフェースに送る復号手段とを備え、

前記制御手段は、前記コピー許諾情報を前記記録手段が再生するように前記記録手段を制御し、

WO 01/48755

PCT/JP00/09260

30

前記復号手段は、前記デバイスユニークキーと前記コピー許諾情報の少なくともいずれかを含む第1の情報を作成し、

前記復号手段は、前記記録ユニット情報を用いて、前記第1の情報を復号した情報であるコンテンツキーを生成し、

前記復号手段は、前記コンテンツキーを用いて前記データを復号することを特徴とする再生装置である。

また、第97の発明は、第7の発明に記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

前記再生されたデータを復号してインターフェースに送る復号手段とを備え、

前記制御手段は、前記暗号化されたタイトルキーを前記記録手段が再生するよう前記記録手段を制御し、

前記復号手段は、前記暗号化されたタイトルキーを前記デバイスユニークキーを用いて復号することを特徴とする再生装置である。

また、第98の発明は、第8の発明に記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

前記再生されたデータを復号してインターフェースに送る復号手段とを備え、

前記復号手段は、前記タイトルキーを用いて前記データを復号することを特徴とする再生装置である。

また、第99の発明は、第9の発明に記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

WO 01/48755

PCT/JP00/09260

31

前記再生されたデータを復号してインターフェースに送る復号手段とを備え、
前記制御手段は、前記暗号化されたタイトルキーを前記記録手段が再生するよ
うに前記記録手段を制御し、

前記復号手段は、前記再生されたタイトルキーを前記デバイスユニークキーを
用いて復号し、

前記復号手段は、前記タイトルキーを含む第3の情報を作成し、

前記制御手段が前記記録手段に連続してアクセスする最小単位である記録ユニ
ットを前提とする記録ブロックに固有の番号及び／または記号である記録ユニ
ット情報を用いて、前記復号手段は、前記第3の情報を復号した情報であるコンテ
ンツキーを生成し、

前記復号手段は、前記コンテンツキーを用いて前記データを復号することを特
徴とする再生装置である。

また、第100の発明は、第10の発明に記載の記録装置によってディスクに
記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

前記再生されたデータを復号してインターフェースに送る復号手段とを備え、

前記復号手段は、前記コピー許諾情報を用いて前記データを復号することを特
徴とする再生装置である。

また、第101の発明は、第11の発明に記載の記録装置によってディスクに
記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

前記再生されたデータを復号してインターフェースに送る復号手段とを備え、

前記制御手段は、前記暗号化されたタイトルキーを前記記録手段が再生するよ

WO 01/48755

PCT/JP00/09260

32

うに前記記録手段を制御し、

前記復号手段は、前記再生されたタイトルキーを前記デバイスユニークキーを用いて復号し、

前記制御手段は、前記コピー許諾情報を前記記録手段が再生するように前記記録手段を制御し、

前記復号手段は、前記タイトルキーと前記コピー許諾情報の少なくともいずれかをを含む第2の情報を作成し、

前記制御手段が前記記録手段に連続してアクセスする最小単位である記録ユニットに対応する記録ブロックに固有の番号及び／または記号である記録ユニット情報を用いて、前記復号手段は、前記第2の情報を復号した情報であるコンテンツキーを生成し、

前記復号手段は、前記コンテンツキーを用いて前記データを復号することを特徴とする再生装置である。

また、第102の発明は、第12または13の発明に記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

前記再生されたデータを復号してインターフェースに送る復号手段とを備え、

前記制御手段は、前記コピー許諾情報を再生するよう前記記録手段を制御し、

前記復号手段は、前記データを前記再生されたコピー許諾情報を用いて復号することを特徴とする再生装置である。

また、第103の発明は、第1～102のいずれかに記載の発明の全部または一部の手段の全部または一部の機能をコンピュータにより実行させるためのプログラム及び／またはデータを担持した媒体であって、コンピュータ

WO 01/48755

PCT/JP00/09260

33

により処理可能なことを特徴とする媒体である。

また、第104の発明は、第1～102のいずれかに記載の発明の全部または一部の手段の全部または一部の機能をコンピュータにより実行させるためのプログラム及び／またはデータであることを特徴とする情報集合体である。

図面の簡単な説明

図1は、本発明の第1、2、4～6の実施の形態におけるハードディスク装置の構成を示すブロック図である。

図2は、本発明の第1の実施の形態におけるハードディスク装置の機能概要を説明する図である。

図3は、本発明の第1の実施の形態におけるハードディスク装置の暗号化手段の構成を示すブロック図である。

図4は、本発明の第1の実施の形態におけるハードディスク装置の復号手段の構成を示すブロック図である。

図5は、(a) 本発明の第1の実施の形態におけるハードディスク装置の記録時の動作を示すフローチャート図である。

(b) 本発明の第1の実施の形態におけるハードディスク装置の記録時の動作の連携を示す模式図である。

図6は、(a) 本発明の第1の実施の形態におけるハードディスク装置の再生時の動作を示すフローチャート図である。

(b) 本発明の第1の実施の形態におけるハードディスク装置の再生時の動作の連携を示す模式図である。

WO 01/48755

PCT/JP00/09260

34

図7は、(a) 本発明の第1の実施の形態におけるハードディスク装置が用いる記録フォーマットを説明する図である。

(b) 上記(a)のフォーマットとは異なるフォーマットの例を示す図である。

図8は、CCIの値とその意味を説明する図である。

図9は、本発明の第1の実施の形態におけるハードディスク装置が記録再生する磁気ディスクのフォーマットを説明する図である。

図10は、本発明の第3の実施の形態におけるハードディスク装置の構成を示すブロック図である。

図11は、本発明の第4の実施の形態におけるハードディスク装置の暗号化手段の構成を示すブロック図である。

図12は、本発明の第4の実施の形態におけるハードディスク装置の復号手段の構成を示すブロック図である。

図13は、本発明の第5の実施の形態におけるハードディスク装置の暗号化手段の構成を示すブロック図である。

図14は、本発明の第5の実施の形態におけるハードディスク装置の復号手段の構成を示すブロック図である。

図15は、本発明の第6の実施の形態におけるハードディスク装置の暗号化手段の構成を示すブロック図である。

図16は、本発明の第6の実施の形態におけるハードディスク装置の復号手段の構成を示すブロック図である。

図17は、(a) 本発明の実施の形態におけるハードディスク装置の暗号化手段の構成を示すブロック図である。

(b) 本発明の実施の形態におけるハードディスク装置の復号手段の構成を示すブロック図である。

WO 01/48755

PCT/JP00/09260

35

すブロック図である。

図18は、(a)本発明の実施の形態におけるハードディスク装置の暗号化手段の構成を示すブロック図である。

(b)本発明の実施の形態におけるハードディスク装置の復号手段の構成を示すブロック図である。

図19は、(a)本発明の実施の形態におけるハードディスク装置の暗号化手段の構成を示すブロック図である。

(b)本発明の実施の形態におけるハードディスク装置の復号手段の構成を示すブロック図である。

図20は、本発明の第7の実施の形態におけるハードディスク装置の構成を示すブロック図である。

図21は、本発明の実施の形態1のAVHDD1およびアーカイブ機器2のブロック図である。

図22は、本発明の実施の形態1のAVHDD12およびアーカイブ機器13のブロック図である。

図23は、本発明の実施の形態1のアーカイブ機器16のブロック図である。

図24は、本発明の実施の形態1のAVHDD19およびアーカイブ機器2のブロック図である。

図25は、本発明の実施の形態2のAVHDD22およびアーカイブ機器23のブロック図である。

図26は、本発明の実施の形態4のAVHDD32およびDVD装置33のブロック図である。

WO 01/48755

PCT/JP00/09260

36

図 27 は、本発明の実施の形態 4 におけるストリームの構成図である。

図 28 は、本発明の実施の形態 1 の、複写手段 80 を備えた AVHDD 81 のブロック図である。

図 29 は、本発明の実施の形態 2 の、複写手段 90 を備えた AVHDD 91 のブロック図である。

図 30 は、本発明の実施の形態 3 の暗号化データ復号記録システムのブロック図である。

図 31 は、本発明の実施の形態 3 の記録装置 100 のブロック図である。

図 32 は、本発明の実施の形態 3 の復号記録装置 101 のブロック図である。

図 33 は、本発明の実施の形態 1 による記録再生装置の構成図である。

図 34 は、本発明の実施の形態 1 による記録再生装置の動作を説明するためのタイムチャートである。

図 35 は、本発明の実施の形態 1 による記録再生装置の動作を説明するためのタイムチャートである。

図 36 は、本発明の実施の形態 2 による記録再生装置の構成図である。

図 37 は、本発明の実施の形態 2 による記録再生装置の動作を説明するためのタイムチャートである。

図 38 は、本発明の実施の形態 2 による記録再生装置の動作を説明するためのタイムチャートである。

図 39 は、本発明の実施の形態 3 による記録再生装置の動作を説明するためのタイムチャートである。

図 40 は、本発明の実施の形態 4 による記録再生装置の構成図である。

WO 01/48755

PCT/JP00/09260

37

図 4 1 は、本発明の実施の形態 5 による記録再生装置の構成図である。

図 4 2 は、本発明の実施の形態 5 による記録再生装置の動作を説明するための図である。

図 4 3 は、従来の技術によるタイムシフト再生を行う記録再生装置の構成図である。

符号の説明

- 1 I E E E 1 3 9 4 バス
- 2 ハードディスク装置
- 3 ホストシステム
- 4 I / F
- 10 コントローラ
- 11 暗号化手段
- 12 復号手段
- 13 デバイスユニークキー
- 14 制御手段
- 15 記録手段
- 16 I / F
- 17 暗号化されたコンテンツ
- 18 秘密領域
- 19 暗号器
- 22 加算器
- 23 タイトルキー

WO 01/48755

PCT/JP00/09260

38

- 2 4 C C I
- 2 5 記録ユニット番号
- 2 6 コンテンツ
- 2 7 C C I
- 2 8 暗号化されたタイトルキー
- 2 9 磁気ディスク媒体
- 3 1 復号器
- 3 2 復号器
- 3 3 復号器
- 3 4 加算器
- 3 5 タイトルキー
- 3 6 C C I
- 3 7 復号されたコンテンツ
- 3 9 記録ユニット
- 4 1 フォーマット
- 4 7 ハードディスク装置
- 5 1 コントローラ
- 1 0 0 1、1 0 1 2、1 0 1 9、1 0 2 2、1 0 3 2 AVHDD
- 1 0 0 2、1 0 1 3、1 0 1 6、1 0 2 3 アーカイブ機器
- 1 0 0 3 S T B
- 1 0 0 4、1 0 2 8 暗号化手段
- 1 0 0 5 第1記録手段
- 1 0 0 6、1 0 2 5、1 0 3 4 蓄積手段

WO 01/48755

PCT/JP00/09260

39

1 0 0 7、1 0 2 7 移動手段
1 0 0 8、1 0 3 1、1 0 3 8 再生手段
1 0 0 9 第2記録手段
1 0 1 0、1 0 2 1 第2の記録媒体
1 0 1 1、1 0 3 5 送信手段
1 0 1 4 バッファ
1 0 1 5 高速送信手段
1 0 1 7 解読再生手段
1 0 1 8 I Cカード
1 0 2 0 判断手段
1 0 2 4 第3記録手段
1 0 2 6 平文化手段
1 0 2 9 第4記録手段
1 0 3 0 第3の記録媒体
1 0 3 3 DVD装置
1 0 3 6 第5記録手段
1 0 3 7 DVD
2 0 1 0 判別情報検出手段
2 0 1 1 時間情報取得手段
2 0 1 2 記録再生手段
2 0 1 3 記録媒体
2 0 1 4 記録バッファ
2 0 1 5 制御入力I/F

WO 01/48755

PCT/JP00/09260

40

2016 切り替え手段

発明を実施するための最良の形態

以下に、本発明の実施の形態を図面を参照して説明する。

(第1の実施の形態)

まず、第1の実施の形態について説明する。

図1に、本発明の記録装置及び再生装置の一実施の形態であるハードディスク装置2の構成を示す。

ハードディスク装置2は、IEEE1394バス1に接続され、さらにIEEE1394バス1は、ホストシステム3に接続されている。

IEEE1394バス1は、AVデータの転送やコマンドのやり取りを中継するIEEE1394-1995に記述されているIEEE standard for High performance Serial Busである。

ホストシステム3は、IEEE1394インターフェースであるI/F16を備えており、ハードディスク装置2に記録させるための著作権保護が必要なデータをIEEE1394バス1に転送したり、ハードディスク装置2からの著作権保護が必要なデータをIEEE1394バス1を介して受信して、再生する装置であり、例えばSTB（セットトップボックス：衛星放送受信器）などである。

ハードディスク装置2は、IEEE1394バス1を介してホストシステム3とAVデータをやり取りしながら、著作権を保護してAVデータを磁気ディスク媒体に記録及び／または磁気ディスク媒体から再生することが出来る装置である。

すなわち、ハードディスク装置2は、図2に示すように磁気ディスク媒体29

WO 01/48755

PCT/JP00/09260

41

に著作権保護が必要なAVデータを暗号化されたコンテンツ17のように暗号化して記録し、また暗号化されたコンテンツ17を再生する装置である。

ハードディスク装置2は、I/F4、コントローラ10、記録手段15から構成される。

また、コントローラ10は、暗号化手段11、復号手段12、デバイスユニークキー13、制御手段14から構成される。

I/F4は、IEEE1394-DTCP (Digital Transmission Content Protection) の方式のインターフェースであり、IEEE1394バス1を介して、ホストシステム3などの外部の機器とコマンドやAVデータをやりとりし、さらに、AVデータを暗号化し、他の機器との認証を行い、認証が成功するか否かに応じて暗号を解読する鍵の無効化をするなどしてIEEE1394バス1上に伝送されるAVデータの著作権を保護することが出来るインターフェースである。

コントローラ10を構成する暗号化手段11は、I/F4から送られてくるAVデータ及びAVデータに付加されたデータを暗号化する手段である。

復号手段12は、記録手段15が読み出したAVデータおよびAVデータに付加されたデータを復号する手段である。

暗号化手段11と復号手段12の構成は後述する。

デバイスユニークキー13は、ハードディスク装置2の一台毎に固有に割り当てられた番号及び／または記号であり、ハードディスク装置2及び／またはコントローラ10の外部からはアクセス出来ない領域に記録されているものである。

記録手段15は、データを記録する磁気ディスク媒体、磁気ディスク媒体に対して情報の記録再生を行う磁気ヘッド、磁気ヘッドを先端に搭載し、磁気ディス

WO 01/48755

PCT/JP00/09260

42

ク媒体の任意の半径位置に位置決め動作を行うアクチュエータ、磁気ディスク媒体を回転させるスピンドルモータなどから構成され、データを磁気ディスク媒体に書き込んだり磁気ディスク媒体からデータを読み出す手段である。記録手段 15 がデータを読み書きする磁気ディスク媒体は、ハードディスク装置 2 に内蔵されており、ハードディスク装置 2 に対して着脱自在ではないものとする。

制御手段 14 は、LBA を指定して、その LBA を記録手段 15 の磁気ディスク媒体のヘッド、セクタに対応付け、アクチュエータ、スピンドルモータを制御して、磁気ヘッドを位置決めし、磁気ヘッドから磁気ディスク媒体に対してデータを書き込んだり読み込んだりするよう制御する手段である。

さて、前述したように図 3 に、暗号化手段 11 の構成を示す。

暗号化手段 11 は、暗号器 19、暗号器 20、暗号器 21、加算器 22 から構成される。

また、図 3 で、デバイスユニークキー 13 は、前述したようにハードディスク装置 2 に割り付けられたハードディスク装置 2 固有の数値及び／または記号である。すなわち、デバイスユニークキー 13 はハードディスク装置 2 の一台毎に異なったものが割り当てられている。また、デバイスユニークキー 13 は、ハードディスク装置 2 のコントローラ 10 内に設けられた秘密領域 18 に記憶されている。この秘密領域 18 は、外部の機器が書き込みも読み出しもできないように保護された領域であり、コントローラ 10 だけが秘密領域 18 に記憶されている情報を読み出すことが出来る領域である。具体的には、この秘密領域 18 は、プリント基板上の ROM を用いて実現することが出来る。すなわち、デバイスユニークキー 13 は、プリント基板上の ROM に記録されている。つまり、この ROM はハードディスク装置 2 及び／またはコントローラ 10 の外部からはアクセス出

WO 01/48755

PCT/JP00/09260

43

来ない。

タイトルキー 23 は、AVデータ毎に固有に割り付けられた数値及び／または記号である。

CCI (Copy control information) 24 は、AVデータに付加されており、コピー許諾情報を表す 2 ビットの数値であり、アイソクロナスパケットのアイソクロナスヘッダの sy 領域に付加されて送られてくるものである。

図 8 に CCI の取り得る値とその意味を示す。CCI が 11 の時、Copy Never を意味する。すなわち、この値の CCI が付加されている AV データを視聴することが出来るが、その AV データをハードディスク装置 2 に記録するなどの複製を作成することを禁止する。

CCI が 10 の時、Copy Once を意味する。すなわち、この値の CCI が付加されている AV データを視聴することが出来、さらにハードディスク装置 2 に記録するなどその AV データの複製一世代だけ作成することが出来る。

CCI が 01 の時、No more Copy を表す。すなわち、CCI が Copy Once である AV データを複製した AV データは No more Copy となる。すなわち、これ以上複製を作成することを禁止することを意味する。つまり、No more Copy は、Copy Once のコンテンツを記録した後、再生時にこれ以上再コピーさせないようにするために必要である。

CCI が 00 の時、Copy Free を意味する。すなわち、この CCI の値が付加されている AV データは自由に視聴することが出来、さらに自由に複製を作成することが出来る。

記録ユニット番号 25 は、制御手段 14 が、記録手段 15 に連続してアクセス

WO 01/48755

PCT/JP00/09260

44

する最小単位である記録ユニットの大きさを持つ記録ブロックに固有の番号及び／または記号である。すなわち上記の異なった記録ブロックには異なった記録ユニット番号 25 が割り当てられている。このような、記録ユニット番号 25 は、ユーザや外部の機器には見えない秘密の情報である。記録ユニット番号 25 と記録ユニットについては後述する。

なお、本実施の形態の記録ユニット番号 25 は、本発明の記録ユニット情報の例である。

コンテンツ 26 は、映画や音楽やドラマなどの番組を構成する AV データである。

また、磁気ディスク媒体 29 は、記録手段 15 によってデータを読み書きされる磁気ディスクである。

暗号器 19 は、秘密領域 18 に記憶されているデバイスユニークキー 13 を読み込み、タイトルキー 23 を暗号化して、暗号化されたタイトルキー 28 を出力する手段である。

加算器 22 は、タイトルキー 23 の下位ビットに続けて CCI 24 を付加した鍵生成用情報を生成する手段である。

なお、本実施の形態の鍵生成用情報は、本発明の第 2 の情報の例である。

暗号器 20 は、鍵生成用情報を記録ユニット番号 25 を用いて暗号化したものであるコンテンツキーを生成する手段である。

暗号器 21 は、コンテンツ 26 をコンテンツキーを用いて暗号化する手段である。

また、図 4 に、復号手段 12 の構成を示す。

復号手段 12 は、復号器 31、復号器 32、復号器 33、加算器 34 から構成

WO 01/48755

PCT/JP00/09260

45

される。

また、図4で、デバイスユニークキー13、タイトルキー35、CCI36、記録ユニット番号25、復号されたコンテンツ37が図示されているが、これらは、それぞれ、図3で示したデバイスユニークキー13、タイトルキー23、CCI24、記録ユニット番号25、コンテンツ26に対応している。

また、磁気ディスク媒体29は、記録手段15によってデータを読み書きされる磁気ディスクであり、図3のものと同一である。

復号器31は、秘密領域18に記憶されているデバイスユニークキー13を読み込み、暗号化されたタイトルキー28をデバイスユニークキー13を用いて復号して、タイトルキー35を出力する手段である。

加算器34は、タイトルキー35の下位ビットに続けてCCI27を付加した鍵生成用情報を生成する手段である。

復号器32は、鍵生成用情報を記録ユニット番号25を用いて復号してコンテンツキーを生成する手段である。

復号器33は、暗号化されたコンテンツ17をコンテンツキーを用いて復号し、復号されたコンテンツ37を出力する手段である。

図7の(a)に、記録手段15の磁気ディスク媒体29の記録フォーマットを示す。磁気ディスク媒体29の領域は、記録ユニットのサイズの複数の記録ブロックである記録ユニット39に分かれている。制御手段14は、記録ユニット39より小さい領域にはアクセス出来ず、また必ず39などの記録ブロックの先頭からアクセスする。すなわち、制御手段14は必ず記録ユニット39の記録ブロック毎にデータを読み込みまたは書き込みを行う。

また、本実施の形態では、一つの記録ユニット39をヘッダ38とデータ40

WO 01/48755

PCT/JP00/09260

46

の領域に分けてAVデータを記録している。

データ40は、トランスポート packets が記録される領域である。またヘッダ38には、暗号化されたタイトルキー35が記録される。記録ユニット39のヘッダ38の領域に記録された情報も、データ40の領域に記録された情報も全て暗号化されている。

すなわち、図7の(b)に記録媒体の記録ブロックにAVデータを記録する別の例を示す。記録ブロック150をヘッダ151とデータ152に分けて記録するのは、本実施の形態の記録フォーマットと同一である。しかし、図7の(b)ではヘッダ151の部分は非暗号化154の部分であり、データ155の部分は暗号化155の部分である。すなわち、データ152の部分のみ暗号化される。従って、IEEE1394バス1などを転送する際に暗号化して転送される鍵153がヘッダ151の部分に暗号化されずに記録されている。従ってヘッダ151の部分に外部の機器が不正にアクセスした場合、鍵153を外部の機器が入手することが出来るので、AVデータの暗号が解読され、その著作権を保護することが出来ないことになる。

これに対して、本実施の形態の記録フォーマットは図7の(a)のように記録ユニット39に記録されるデータを全て暗号化しているので、著作権を図7の(b)のような記録フォーマットに較べてより確実に保護することが出来る。

このように、本実施の形態の記録フォーマットは、ハードディスク装置を製造するメーカーに固有のものである。このため、標準的なフォーマットを採用している外部の機器からは、このようなメーカーに固有のフォーマットで記録されているデータを読み取ることは困難である。従って、本実施の形態の記録フォーマットを用いることによって、磁気ディスク媒体29に記録されているAVデータの著

WO 01/48755

PCT/JP00/09260

47

作権を保護することが出来る。また、本実施の形態の記録フォーマットのセクタサイズや記録ユニットのサイズは自由に設計することが出来る。

記録ユニットの具体例としては、例えば磁気ディスク媒体29のセクタがある。すなわち、1セクタ、連続する62セクタ、連続する128セクタ、・・・連続する2048セクタなど、連続する所定の個数のセクタを記録ユニット39とすることが出来る。

また、前述した記録ユニット番号25の具体例としては、例えばセクタのLBA (Logical block address) を記録ユニット番号25とすることが出来る。すなわち、記録ユニット39の先頭のセクタのLBA、記録ユニット39の先頭から2番目のセクタのLBA、記録ユニット39の先頭からN番目 (Nは記録ユニットを構成するセクタの総数以下の整数) のいずれかを記録ユニット番号25とすることが出来る。

あるいは、記録ユニット39を一意に特定するための番号を使用することも出来る。すなわち、記録ユニット39を磁気ディスク媒体29の内周から外周に向かう順番に数えた場合の番号を記録ユニット番号25とすることが出来る。

あるいは、記録ユニットを管理するために使用する内部管理用のアドレスを使用することも出来る。

あるいは、これらの複数通りの例を所定の規則に従って組み合わせて生成した数値や記号を用いてもよい。

要するに記録ユニット番号25としては、ユーザからは見えない情報であり、磁気ディスク媒体29の全ての記録ユニット39を重複なく一意に特定する情報でありさえすればよい。

なお、本実施の形態のハードディスク装置2は本発明の記録装置の例であり、

WO 01/48755

PCT/JP00/09260

48

本実施の形態のハードディスク装置 2 は本発明の再生装置の例でもあり、本実施の形態の記録手段は本発明の再生手段の例を兼ねている。

さらに、本実施の形態の I / F 4 は本発明のインターフェースの例であり、本実施の形態の磁気ディスク媒体 2 9 は本発明のディスクの例である。

また、暗号化手段 1 1、復号手段 1 2 及びデバイスユニークキー 1 3 を含むコントローラ 1 3 と、I / F 4 は一枚のプリント基板上に一体化して配設されている。また、暗号化手段 1 1、復号手段 1 2、制御手段 1 4、I / F 4 はそれぞれ 1 チップの L S I として実装されている。これらのチップの端子における信号は、公開されていないフォーマットに従ってビットの並べ替えなどのスクランブルが施されている。従って、これらの端子から A V データとして再生出来る信号を外部の機器が取り出しても、信号を作成したフォーマットが解らないので、A V データとして再生することは容易でない。

次に、このような本実施の形態の動作を説明する。

まず、ハードディスク装置 2 が著作権保護を必要とする A V データを記録する場合の動作を説明する。

なお、本実施の形態では、A V データは、M P E G 2 トランスポートストリーム形式で送られてくる。

図 5 の (a) にホストシステム 3、ハードディスク装置 2 の主な動作をフローチャートで示す。以下、このフローチャートに従って説明する。また、図 5 の (b) にホストシステム 3、ハードディスク装置 2 の動作の連携を模式図を用いて示す。

ホストシステム 3 は、著作権保護を必要とする A V データを暗号化し、アイソクロナスパケットとして I E E E 1 3 9 4 バス 1 に伝送している。

WO 01/48755

PCT/JP00/09260

49

I/F 16は、MPEG 2トランスポートストリーム形式のAVデータを暗号化する。さらに、暗号化されたMPEG 2トランスポートストリームのトランスポートパケットにソースパケットヘッダを付加してソースパケットを作成する。そして、ソースパケットを分割または結合したデータブロックにCIPヘッダを付加して、CIPを作成する。さらに、CIPにアイソクロナスヘッダを付加してアイソクロナスパケットを作成し、IEEE 1394バス1に伝送する。

また、アイソクロナスパケットを生成する際に、図3のCCI 24は、アイソクロナスパケットのsy領域に付加される。

ホストシステム3は、ハードディスク装置2にAVデータの記録を開始するコマンドを発行したとする。

このコマンドは、I/F 16からアシンクロナスパケットとして、IEEE 1394バス1を経由してI/F 4に送られる。

I/F 4は記録開始を指示するコマンドを受信すると、I/F 16に認証を要求する。

これを受けてI/F 16とI/F 4は認証動作を行う(S1)。図5の(b)ではこの認証動作を認証85で表した。

I/F 16は、ハードディスク装置2がAVデータを記録するのに適正な機器か不正な機器かを判断する。適正な機器であれば認証が成功し、不正な機器であれば認証が失敗する(S2)。

ハードディスク装置2がAVデータを記録する資格がない場合は、認証が失敗する(S3)。この場合ハードディスク装置2はAVデータを記録することが出来ない。

ハードディスク装置2がAVデータを記録することが出来る適正な機器である

WO 01/48755

PCT/JP00/09260

50

場合、認証は成功する。

認証が成功すると、I/F 4は、ホストシステム3が伝送しているアイソクロナスパケットをそのアイソクロナスチャンネルを識別して受信する。

そして、I/F 4は、受信したアイソクロナスパケットのアイソクロナスヘッダからCCIを分離する。

そして、CCIの値によって以下の動作を行う。

すなわち、図8において、CCIが11の時、すなわちCopy Neverの場合、AVデータを記録することが許可されていないので、I/F 4は、記録処理をしないことをホストシステム3に通知し、コントローラ10に記録処理を開始するよう指示しない。

CCIが10の時、すなわち、Copy Onceの場合、I/F 4は、記録処理を開始することをホストシステム3に通知し、さらにコントローラ10に記録処理を開始するように指示する。

CCIが01の時、すなわち、No more Copyの場合、I/F 4は、CCIがCopy Neverと同様の動作を行う。

CCIが00の時、すなわち、Copy Freeの場合、記録処理を開始することをホストシステム3に通知し、さらにコントローラ10に記録処理を開始するように指示する。

従って、CCIが10の場合、I/F 4は、認証動作の際にホストシステム3から受け取った鍵で暗号化されているAVデータを復号する。そして、復号したAVデータを、トランスポートパケット毎にソースパケットヘッダに付加されていた伝送用タイムスタンプの指示するタイミングで、トランスポートパケット毎に出力する。CCIが00の場合、AVデータは暗号化されずに送られてくるの

WO 01/48755

PCT/JP00/09260

51

で、復号処理をせず、伝送用タイムスタンプの指示するタイミングで、トランスポート packets 毎に出力する。

このように、I/F 4 から出力される AV データは復号され平文となっているが、ハードディスク装置 2 独自のフォーマットで記述された信号で出力されるので、第 3 者が I/F 4 のチップの端子から信号を取り出しても、第 3 者が利用出来る AV データに復元することは非常に困難である。

暗号化手段 11 は、I/F 4 から送られてくる MPEG 2 トランスポート packets を入力する。

まず、暗号器 19 は、秘密領域 18 に記憶されているデバイスユニークキー 13 を読み込む (S4)。

暗号化手段 11 は、I/F 4 から送られてきた AV データに付加されているタイトルキー 23 を検出する。そして、暗号器 19 は、検出したタイトルキー 23 をデバイスユニークキー 13 によって暗号化する (S5)。

次に、暗号器 19 が暗号化したタイトルキー 23 は、制御手段 14 の制御に従って、記録手段 15 の磁気ディスク媒体 29 に暗号化されたタイトルキー 28 のように記録される (S6)。この暗号化されたタイトルキー 28 を、図 5 の (b) にも示す。

さらに、暗号化手段 11 は、AV データに付加されて送られてきた CCI 24 を検出する。検出された CCI 24 は、制御手段 14 の制御に従って、記録手段 15 の磁気ディスク媒体 29 に CCI 27 として記録される。

加算器 22 は、タイトルキー 23 の下位ビットに続けて CCI 24 を付加した情報である鍵生成用情報を生成する。

一方、制御手段 14 から AV データの付加情報としてどの記録ユニットに AV

WO 01/48755

PCT/JP00/09260

52

データを記録するかの情報も送られてきている。暗号化手段 11 は、記録する記録ユニットの記録ユニット番号 25 を求める。

暗号器 20 は、AV データを記録しようとしている記録ユニットの記録ユニット番号 25 を用いて、加算器が生成した鍵生成用情報を暗号化する。この暗号化した情報のことをコンテンツキーと呼ぶことにする。コンテンツキーは、記録ユニット番号 25 で暗号化したので、記録ユニット毎に変化する。

次に、暗号器 21 は、これから記録する AV データであるコンテンツ 26 をコンテンツキーで暗号化する (S7)。

暗号化された AV データは、制御手段 14 の制御に従って、記録手段 15 の磁気ディスク媒体 29 の記録すべき記録ユニットに暗号化されたコンテンツ 17 として、記録される (S8)。図 5 の (b) にも暗号化されたコンテンツ 17 を示す。

以下、同様に、鍵生成用情報を、記録ユニット毎に、記録ユニット番号 25 で暗号化してコンテンツキーを生成し、生成したコンテンツキーでコンテンツ 26 を暗号化し (S7)、暗号化したコンテンツ 17 を磁気ディスク媒体 29 に記録する (S8) という動作を繰り返す。

このようにして、ハードディスク媒体 29 は、著作権保護の必要な AV データを磁気ディスク媒体 29 に記録する。

次に、ハードディスク装置 2 が著作権保護を必要とする AV データを再生する場合の動作を説明する。

図 6 の (a) にホストシステム 3、ハードディスク装置 2 の再生時の主な動作をフローチャートで示す。以下、このフローチャートに従って説明する。また、図 6 の (b) にホストシステム 3、ハードディスク装置 2 の再生時の主な動作の

WO 01/48755

PCT/JP00/09260

53

連携を説明する模式図を示す。

ホストシステム 3 がハードディスク装置 2 に再生開始を指示するコマンドを発行したとする。

このコマンドは、I/F 16 からアシンクロナスパケットとして、IEEE 1394 バス 1 を経由して I/F 4 に送られる。

さらに、I/F 16 は、I/F 4 に対して認証要求を行う。

これを受けて I/F 16 と I/F 4 は認証動作を行う (S 9)。この認証動作は、図 6 の (b) では認証 86 として示されている。

I/F 4 は、ホストシステム 3 が AV データを利用するのに適正な機器が不正な機器かを判断する。適正な機器であれば認証が成功し、不正な機器であれば認証が失敗する (S 10)。

ホストシステム 3 が AV データを利用する資格がない場合は、認証が失敗する (S 11)。この場合、ホストシステム 3 は、AV データを記録することが出来ない。

ホストシステム 3 が AV データを記録することが出来る適正な機器である場合、認証は成功する。

認証が成功すると、I/F 4 は、AV データを再生するコマンドが送られてきたことをコントローラ 10 に通知する。

復号手段 12 は、この通知を受け取ると、まず、復号器 31 は、秘密領域 18 に記憶されているデバイスユニークキー 13 を読み込む (S 12)。

さらに、制御手段 14 の制御に従って、記録手段 15 が暗号化されたタイトルキー 28 を磁気ディスク媒体 29 から読み出す (S 13)。図 6 の (b) にも暗号化されたタイトルキー 28 を示す。

WO 01/48755

PCT/JP00/09260

54

復号器 31 は、デバイスユニークキー 13 によって、暗号化されたタイトルキー 28 を復号する (S14)。そして、復号手段 12 は、復号されたタイトルキー 35 を I/F4 に転送する。

制御手段 14 の制御に従って、記録手段 15 は、磁気ディスク媒体 29 から CCI27 を読み出す。

復号手段 12 は、CCI27 を I/F4 に転送する。

加算器 34 は、復号されたタイトルキー 35 の下位ビットに続けて読み出した CCI27 を付加した情報である鍵生成情報を生成する。

制御手段 14 は、読み取るべき記録ユニット 39 を指定して、記録手段 15 が記録ユニット 39 に格納されている情報である暗号化されたコンテンツ 17 を読み取るよう制御する。

復号手段 12 は、記録ユニット 39 の記録ユニット番号 25 を求める。

復号器 32 は、データを読み出そうとしている記録ユニット 39 の記録ユニット番号 25 を用いて、加算器が生成した鍵生成用情報を復号する。この復号した情報のことをコンテンツキーと呼ぶことにする。コンテンツキーは、記録ユニット番号 25 で復号したので、記録ユニット毎に変化する。

次に、制御手段 14 の制御に従って、記録手段 15 は、磁気ディスク媒体 29 の読み出すべき記録ユニットに格納されている情報である暗号化されたコンテンツ 17 を読み出す (S15)。図 6 の (b) にも暗号化されたコンテンツ 17 を示す。

次に、復号器 33 は、記録手段 15 が読み出した暗号化されたコンテンツ 17 をコンテンツキーで復号する (S16)。

復号手段 12 は、復号されたコンテンツ 37 を I/F4 に転送する。

WO 01/48755

PCT/JP00/09260

55

以下、同様に、鍵生成用情報を、記録ユニット毎に、記録ユニット番号25で復号してコンテンツキーを生成し、暗号化されたコンテンツ17を読み出し(S15)、暗号化されたコンテンツ17を、コンテンツキーで復号し(S16)、復号したコンテンツ27をMPEG2トランスポートストリームとしてI/F4に転送するという動作を繰り返す。

また、復号手段12から出力されるAVデータは復号されているが、ハードディスク装置2独自のフォーマットで記述された信号であるので、第3者が復号手段12のチップの端子から信号を取り出しても、第3者が利用出来るAVデータに復元することは非常に困難である。

I/F4はコントローラ10から送られてきたAVデータを暗号化する。そして、アイソクロナスパケットとしてIEEE1394バス1に転送する。

ホストシステム3のI/F16は、アイソクロナスチャンネルを識別して、アイソクロナスパケットを受信し、暗号化されているAVデータを復号する。

I/F16は、受信したAVデータをMPEG2トランスポートストリームとして出力する。

出力されたAVデータはホストシステム3の有する図示していないトランスポートストリームデコーダで分離される。そして、図示していないAVデコーダがAVデコードしてアナログ信号に変換し、モニタに表示する。

このようにして、ハードディスク媒体29は、著作権保護の必要なAVデータを磁気ディスク媒体29から再生する。

本実施の形態のハードディスク装置2は、AVデータの記録時、AVデータの再生時、及び記録手段15にAVデータが記録済みのいずれの場合でも、著作権保護が必要なAVデータの著作権を保護することが出来る。

WO 01/48755

PCT/JP00/09260

56

なお、本実施の形態では、磁気ディスク 29 がハードディスク装置 2 から着脱できないとして説明したが、これに限らず着脱自在であっても構わない。

さらに、本実施の形態では、デバイスユニークキー 13 がハードディスク装置 2 のプリント基板上の秘密領域 18 としての ROM に記憶されているとして説明したが、これに限らない。秘密領域 18 を磁気ディスク媒体 29 に設けても構わない。すなわち、デバイスユニークキー 13 を磁気ディスク 29 のユーザのアクセス出来ない領域に記憶しても構わない。

さらに、本実施の形態では、暗号化されたタイトルキー 28 を磁気ディスク 29 のユーザがアクセス出来るユーザ領域に記録するとして説明したが、これに限らない。ディスク媒体 29 のユーザがアクセス出来ないシステム領域に記録しても構わない。また、ハードディスク装置 2 のプリント基板上に設けられた RAM に記録しても構わない。

さらに、本発明の記録装置及び再生装置は、本実施の形態では、ハードディスク装置 2 として一体化されているとして説明したがこれに限らない。本発明の記録装置が、I/F 4、暗号化手段 11、制御手段 14、記録手段 15 から構成されており、AV データを記録する装置であり、また、本発明の再生装置が、I/F 4、復号手段 12、制御手段 14、記録手段 15 から構成されているなど、要するに本発明の記録装置は、暗号化手段と制御手段と記録手段を備えていさえすればよい。また、本発明の再生装置は、復号手段、制御手段を備えていさえすればよい。

さらに、本実施の形態のハードディスク装置 2 の I/F 4、暗号化手段 11、復号手段 12、制御手段 14 はそれぞれ 1 チップの LSI で構成されているとして説明したが、これに限らない。I/F 4、暗号化手段 11、復号手段 12、制

WO 01/48755

PCT/JP00/09260

57

御手段 14 がそれぞれ複数チップの L S I から構成されていても構わない。また、チップの端子では、A V データは非公開のフォーマットで記述されているとして説明したがこれに限らず、端子間を伝送するために暗号化されていても構わない。また、チップの端子の性質が非公開のフォーマットで定められていても構わない。なお、ここでチップの端子の性質とは、どの端子がどのような信号を出力するか、またどの端子とどの端子とが組になってどのような信号を出力するか、また各端子がどのような用途に用いられるかなどの性質を表すものである。このようなチップの端子の性質が非公開のフォーマットで定められているため、例えば各端子がどのような用途に用いられるかなどをユーザが知ることが出来ないものである。要するに、I / F 4、コントローラ 10 が配設されているプリント基板上の端子及びチップの端子のうち、第 3 者が A V データとして再生出来る信号を出力している端子で検出される信号は、全て暗号化されているか及び／または非公開のフォーマットで記述されているか、またはそれらの端子の性質が非公開のフォーマットで定められていさえすればよい。

さらに、本実施の形態のハードディスク装置 2 の I / F 4、暗号化手段 11、復号手段 12、制御手段 14 が 1 チップの L S I で構成されていても構わない。このようにすればさらに A V データの著作権を確実に保証することが出来る。

さらに、本実施の形態では、C C I を用いて A V データを暗号化するとして説明したが、これに限らない。C C I を用いずに A V データを暗号化しても構わない。すなわち、加算器 22 が、C C I とタイトルキー 23 から鍵生成用情報を作成する代わりに、加算器 22 を用いず、タイトルキー 23 を直接鍵生成用情報とし、この鍵生成用情報を記録ユニット番号で暗号化してコンテンツキーを生成しても構わない。なお、この場合のタイトルキー 23 は本発明の第 3 の情報の例で

ある。このように、CCIを用いずにAVデータを暗号化する場合、本実施の形態のようにCCIを磁気ディスク媒体29に記録しても構わないし、また、CCIを磁気ディスク媒体29に記録しなくても構わない。

さらに、本実施の形態では、ハードディスク装置2がAVデータに付加されているCCIの値がCopy neverの場合、そのAVデータを記録せず、CCIの値がCopy onceの場合、そのAVデータを暗号化して記録し、CCIの値がNo more copyの場合、そのAVデータを記録せず、CCIの値がCopy freeの場合、そのAVデータを暗号化して記録するとして説明したが、これに限らない。AVデータに付加されているCCIの値がいずれの値を取る場合であってもAVデータを暗号化して記録しても構わない。あるいは、AVデータに付加されているCCIの値がCopy freeの場合、そのAVデータを暗号化しないで平文のまま記録しても構わない。

さらに、本実施の形態では、鍵生成用情報は、復号されたタイトルキーの下位ビットに続けて読み出したCCIを付加した情報であるとして説明したがこれに限らない。鍵生成用情報として、タイトルキーの上位ビットの前に読み出したCCIを付加した情報であっても構わない。さらに、鍵生成用情報は、タイトルキーとCCIのみを含む情報であっても構わないし、タイトルキーとCCIを含み、さらにそれ以外の情報が含まれていても構わない。また、タイトルキーとCCIのいずれか一方を含む情報であっても構わない。要するに本実施の形態の鍵生成用情報は、タイトルキーとCCIの少なくともいずれかを含む情報でありさえすればよい。

(第2の実施の形態)

次に、第2の実施の形態について説明する。

WO 01/48755

PCT/JP00/09260

59

本実施の形態では、CCIの処理を中心に説明する。

図1に、本発明の記録装置及び再生装置の一実施の形態であるハードディスク装置2の構成を示す。

本実施の形態のハードディスク装置2の構成は第1の実施の形態と同一である。

図9に、記録手段15の磁気ディスク媒体29のフォーマット41を示す。紙面左側が磁気ディスク媒体29のディスク内周45であり、紙面右側がディスク外周46に対応している。ディスク内周45側の領域は、システムFAT42であり、ディスク外周46側は、データ43である。

システムFAT42は、ユーザがアクセス出来ないシステム領域であり、ファイル管理情報など、制御手段14がシステムを制御するために使用する領域である。

一方データ43は、ユーザがアクセス出来る領域であり、AVデータが記録されている。すなわち、図3、図4で示すような、暗号化されたコンテンツ17、暗号化されたタイトルキー28などが記録されている。

そして、CCIはCCIデータ44に示すようにシステムFAT42にデータ43を構成する記録ユニット毎に記録される。すなわち、記録ユニット毎にCCIの値が割り付けられている。

また、ファイル管理情報とは、例えばFAT (file allocation Table) とディレクトリと呼ばれる情報からなる。

FATは、記録ユニットのアドレスと次の記録ユニットのアドレスが対になったテーブルであり、ファイルのデータがどのような記録ユニットにどのような順番で格納されているかを示すものである。

また、ディレクトリは、ファイルを階層的に管理するテーブルであり、ファイ

WO 01/48755

PCT/JP00/09260

60

ル名とファイルに格納されているデータが格納されている先頭の記録ユニットのアドレスと、ファイルが読み込み専用か、重ね書き可能かなどの属性を示す情報が対になったテーブルである。

FATとディレクトリを用いれば、ファイルの作成、編集、消去などの処理を管理することが出来る。

次に、このような本実施の形態の動作を説明する。

第1の実施の形態と同様にしてハードディスク装置2は、AVデータを記録している。このとき、AVデータは第1の実施の形態と同様にして次々と記録ユニット毎に記録されていく。新しい記録ユニットにAVデータの記録が完了する毎に、AVデータがどの記録ユニットに記録されたかを示すファイル管理情報を制御手段14が作成、更新していく。そしてこのファイル管理情報を自らのメモリに保持していく。

そして、AVデータの記録がすべて完了したタイミングで、制御手段14は、作成、更新したファイル管理情報をシステムFAT42に書き込み、システムFAT42を最新のものに更新する。

最後に制御手段14は、AVデータが新規に書き込まれた記録ユニットのCCIの値をファイル管理情報に書き込む。

このように、AVデータを記録する際、まず、AVデータが磁気ディスク媒体29に記録され、AVデータの記録が完了してから管理情報が磁気ディスク媒体29に記録され、最後にCCIがシステムFAT42に書き込まれる。

ところで、AVデータを記録中にユーザがハードディスク装置2の電源コンセントを誤って抜きとり、ハードディスク装置2の電源を切ってしまったとする。このような場合、すでに記録中であったAVデータのすでに記録された部分のフ

WO 01/48755

PCT/JP00/09260

61

ファイル管理情報とCCIは消えてしまう。

本実施の形態のハードディスク装置2は、このように記録が中断されたAVデータを次のようにして再生する。

制御手段14は、磁気ディスク29の空の記録ユニットに書き込む順番を所定の規則に従って決めている。

制御手段14は、記録が中断されたAVデータをこの規則に従って記録されているとして、更新前のファイル管理情報から再生する。そして、暗号化手段11は、CCI 2ビット分の値の組み合わせで復号を試みる。

そして、復号に成功したCCIの値でさらに、最初からAVデータを復号する。

このように本実施の形態のハードディスク装置2は、記録が中断されたAVデータを正常に復号することが出来る。

さらに、AVデータの終端は、トランスポート packets に付加されているPCRの値の連続性から検出する。

すなわち、PCRは、長くとも100msの間隔でトランスポート packets に付加されており、PCRの値は、27MHzの周波数でカウントアップする上位33ビット、下位9ビットのカウンタ値である。従って、PCRの値が100ms以上に相当する値以上に変化すれば、AVデータの終端を超えて別のAVデータを再生してしまったことがわかる。従って、暗号化手段11は、PCRの値が連続である範囲のAVデータのみをI/F4に転送する。

なお、本実施の形態のハードディスク装置2は、第1の実施の形態と同様にして暗号化および復号を行うとして説明したがこれに限らない。第1の実施の形態とは別の暗号化を行っても構わない。要するにCCIを用いて暗号化を行うハードディスク装置でありさえすればよい。

WO 01/48755

PCT/JP00/09260

62

さらに本実施の形態のハードディスク装置 2 は、CCI の値を仮定して復号を試行するとして説明したがこれに限らない。AV データを記録する前に CCI を磁気ディスク 29 に記録し、AV データの記録が中断しても必ず CCI が記録手段 15 に記録されるようにしても構わない。

さらに、本発明の記録装置及び再生装置は、本実施の形態では、ハードディスク装置 2 として一体化されているとして説明したがこれに限らない。本発明の記録装置が、I/F 4、暗号化手段 11、制御手段 14、記録手段 15 から構成されており、AV データを記録する装置であり、また、本発明の再生装置が、I/F 4、復号手段 12、制御手段 14、記録手段 15 から構成されているなど、要するに本発明の記録装置は、暗号化手段と制御手段と記録手段を備えていさえすればよい。また、本発明の再生装置は、復号手段、制御手段を備えていさえすればよい。

さらに、本実施の形態では、ファイル管理情報は、FAT とディレクトリからなるとして説明したがこれに限らない。OS/2 における HPFS (high performance file system)、Mac OS のファイルシステム、UNIX における i ノード、Windows 95 における VFAT (virtual FAT)、Windows NT の NTFS (new technology file system) などにおけるファイル管理情報を用いても構わない。ただし、その場合、第 1 の実施の形態で説明した記録ユニットを、これらのファイル管理情報の記録ブロックに一致させておく必要がある。要するにハードディスクに対して記録再生が可能な OS におけるファイル管理情報を用いても構わない。

(第 3 の実施の形態)

WO 01/48755

PCT/JP00/09260

63

次に、第3の実施の形態について説明する。

図10に本発明の記録装置及び再生装置の一実施の形態であるハードディスク装置47の構成を示す。

本実施の形態のハードディスク装置47は、第1の実施の形態のI/F4の代わりにI/F48を備えている。また、本実施の形態のコントローラ51は、暗号化手段11、復号手段12、デバイスユニークキー13を持たない。

I/F48は、IEEE1394バス1から送られてくる暗号化されたAVデータを復号せず、コントローラ51に転送し、またコントローラ51から送られてくる暗号化されたAVデータをそのままIEEE1394バス1に転送するインターフェースである。それ以外は、第1の実施の形態のI/F4と同一である。

次に、このような本実施の形態のハードディスク装置47の動作を第1の実施の形態との相違点を中心に説明する。

まず、AVデータを記録する際の動作を説明する。

第1の実施の形態と同様にして、I/F16とI/F48が認証動作を行い、認証が成功したとする。そうすると、I/F48はアイソクロナスチャンネルを識別してホストシステム3から送られてくるアイソクロナスパケットを受信する。

そして、アイソクロナスパケットからMPEG2トランスポートストリームを復元する。そして、トランスポートパケットを順次コントローラ51に転送する。

制御手段14は、暗号化されているAVデータを記録手段15が磁気ディスク29に記録するように制御する。

それ以外は、第1の実施の形態と同一である。

このように本実施の形態のハードディスク装置47は、暗号化されているAVデータをそのまま記録する。

WO 01/48755

PCT/JP00/09260

64

次に、暗号化されているAVデータを再生する際の動作を説明する。

第1の実施の形態と同様にして、I/F16とI/F48が認証動作を行い、認証が成功したとする。そうすると、制御手段14は、記録手段15が暗号化されているAVデータを読み出すように制御する、そしてコントローラ51は、読み出したAVデータをMPEG2トランスポートストリームとしてI/F48に転送する。

I/F48は、暗号化されているMPEG2トランスポートストリームをアイソクロナスパケットとしてIEEE1394バス1に転送する。

それ以外は第1の実施の形態と同一である。

このように、本実施の形態のハードディスク装置47は伝送用に暗号化されたAVデータをそのまま記録及び再生することによって簡易な構成で、AVデータの著作権を保護することが出来る。

(第4の実施の形態)

次に、第4の実施の形態について説明する。

図1に、本発明の記録装置及び再生装置の一実施の形態であるハードディスク装置2を示す。本実施の形態のハードディスク装置2は、第1の実施の形態で説明したハードディスク装置2の暗号化手段11と復号手段12の代わりに別の暗号化手段と復号手段に置き換えたものである。

図11に本実施の形態のハードディスク装置2の暗号化手段60を示す。また、図12に本実施の形態の復号手段61を示す。

本実施の形態では、第1の実施の形態との相違点である暗号化手段60と復号手段61を中心に説明する。

図11において、暗号化手段60は、暗号器19、暗号器52、暗号器21か

WO 01/48755

PCT/JP00/09260

65

ら構成される。すなわち、暗号化手段 60 は、第 1 の実施の形態の暗号化手段 11 とは異なり、CCI を用いて暗号化しない。

すなわち、暗号器 19 は、秘密領域 18 に記憶されているデバイスユニークキー 13 を読み込み、タイトルキー 23 を暗号化して、暗号化されたタイトルキー 28 を出力する手段である。

なお、本実施の形態のタイトルキー 23 は、本発明の第 1 の情報の例である。

暗号器 52 は、タイトルキー 23 を記録ユニット番号 25 を用いて暗号化したものであるコンテンツキーを生成する手段である。

暗号器 21 は、コンテンツ 26 をコンテンツキーを用いて暗号化する手段である。

図 12 に本実施の形態のハードディスク装置 2 の復号手段 61 を示す。

図 12 において、復号手段 61 は、復号器 31、復号器 53、復号器 33 から構成される。復号手段 61 は、第 1 の実施の形態とは異なり CCI を復号に用いない。

すなわち、復号器 31 は、秘密領域 18 に記憶されているデバイスユニークキー 13 を読み込み、暗号化されたタイトルキー 28 をデバイスユニークキー 13 を用いて復号して、タイトルキー 35 を出力する手段である。

なお、本実施の形態のタイトルキー 28 は本発明の第 2 の情報の例である。

復号器 53 は、タイトルキー 35 を記録ユニット番号 25 を用いて復号してコンテンツキーを生成する手段である。

復号器 33 は、暗号化されたコンテンツ 17 をコンテンツキーを用いて復号し、復号されたコンテンツ 37 を出力する手段である。

次に、このような本実施の形態の動作を第 1 の実施の形態との相違点である暗

WO 01/48755

PCT/JP00/09260

66

号化手段60と復号手段61の動作を中心に説明する。

まず、暗号化手段60の動作を説明する。

暗号器19は、秘密領域18に記憶されているデバイスユニークキー13を読み込む。

暗号化手段60は、I/F4から送られてきたAVデータに付加されているタイトルキー23を検出する。そして、暗号器19は、検出したタイトルキー23をデバイスユニークキー13によって暗号化する。

次に、暗号器19が暗号化したタイトルキー23は、制御手段14の制御に従って、記録手段15の磁気ディスク媒体29に暗号化されたタイトルキー28のように記録される。

さらに、暗号化手段60は、AVデータに付加されて送られてきたCCI24を検出する。検出されたCCI24は、制御手段14の制御に従って、記録手段15の磁気ディスク媒体29にCCI27として記録される。

暗号化手段60は、記録する記録ユニットの記録ユニット番号25を求める。

暗号器52は、AVデータを記録しようとしている記録ユニットの記録ユニット番号25を用いて、タイトルキー23を暗号化する。この暗号化した情報のことをコンテンツキーと呼ぶことにする。コンテンツキーは、記録ユニット番号25で暗号化したので、記録ユニット毎に変化する。

次に、暗号器21は、これから記録するAVデータであるコンテンツ26をコンテンツキーで暗号化する。

暗号化されたAVデータは、制御手段14の制御に従って、記録手段15の磁気ディスク媒体29の記録すべき記録ユニットに暗号化されたコンテンツ17として、記録される。

WO 01/48755

PCT/JP00/09260

67

以下、同様に、タイトルキー 23 を、記録ユニット毎に、記録ユニット番号 25 で暗号化してコンテンツキーを生成し、生成したコンテンツキーでコンテンツ 26 を暗号化し、暗号化したコンテンツ 17 を磁気ディスク媒体 29 に記録するという動作を繰り返す。

このようにして、ハードディスク媒体 29 は、著作権保護の必要な AV データを磁気ディスク媒体 29 に記録する。

次に、復号手段 61 の動作を説明する。

復号器 31 は、秘密領域 18 に記憶されているデバイスユニークキー 13 を読み込む。

さらに、制御手段 14 の制御に従って、記録手段 15 が暗号化されたタイトルキー 28 を磁気ディスク媒体 29 から読み出す。

復号器 31 は、デバイスユニークキー 13 によって、暗号化されたタイトルキー 28 を復号する。そして、復号手段 61 は、復号されたタイトルキー 35 を I/F 4 に転送する。

制御手段 14 の制御に従って、記録手段 15 は、磁気ディスク媒体 29 から CCI 27 を読み出す。

復号手段 12 は、CCI 27 を I/F 4 に転送する。

制御手段 14 は、読み取るべき記録ユニット 39 を指定して、記録手段 15 が記録ユニット 39 に格納されている情報である暗号化されたコンテンツ 17 を読み取るよう制御する。

復号手段 61 は、記録ユニット 39 の記録ユニット番号 25 を求める。

復号器 53 は、データを読み出そうとしている記録ユニット 39 の記録ユニット番号 25 を用いて、タイトルキー 35 を復号する。この復号した情報のことを

WO 01/48755

PCT/JP00/09260

68

コンテンツキーと呼ぶことにする。コンテンツキーは、記録ユニット番号 25 で復号したので、記録ユニット毎に変化する。

次に、制御手段 14 の制御に従って、記録手段 15 は、磁気ディスク媒体 29 の読み出すべき記録ユニットに格納されている情報である暗号化されたコンテンツ 17 を読み出す。

次に、復号器 33 は、記録手段 15 が読み出した暗号化されたコンテンツ 17 をコンテンツキーで復号する。

復号手段 61 は、復号されたコンテンツ 37 を I/F 4 に転送する。

以下、同様に、タイトルキー 35 を、記録ユニット毎に、記録ユニット番号 25 で復号してコンテンツキーを生成し、暗号化されたコンテンツ 17 を読み出し、暗号化されたコンテンツ 17 を、コンテンツキーで復号し、復号したコンテンツ 27 を MPEG 2 トランスポートストリームとして I/F 4 に転送するという動作を繰り返す。

本実施の形態で説明した暗号化手段 60 と復号手段 61 をハードディスク装置 2 に用いることにより、第 1 の実施の形態と同等の効果が得られる。

また、暗号化手段 60 と復号手段 61 を第 1 の実施の形態で説明した種々の変形例に適応出来ることは言うまでもない。

(第 5 の実施の形態)

次に、第 5 の実施の形態について説明する。

図 1 に、本発明の記録装置及び再生装置の一実施の形態であるハードディスク装置 2 を示す。本実施の形態のハードディスク装置 2 は、第 1 の実施の形態で説明したハードディスク装置 2 の暗号化手段 11 と復号手段 12 の代わりに別の暗号化手段と復号手段に置き換えたものである。

WO 01/48755

PCT/JP00/09260

69

図 1 3 に本実施の形態のハードディスク装置 2 の暗号化手段 6 2 を示す。また、図 1 4 に本実施の形態の復号手段 6 3 を示す。

本実施の形態では、第 1 の実施の形態との相違点である暗号化手段 6 2 と復号手段 6 3 を中心に説明する。

図 1 3 において、暗号化手段 6 2 は、加算器 5 4、暗号器 5 5、暗号器 2 1 から構成される。本実施の形態の暗号化手段 6 2 は、暗号化手段 1 1 とは異なり、AV データの暗号化にタイトルキーを用いない。

すなわち、加算器 5 4 は、デバイスユニークキー 1 3 の下位ビットに続けて C I 2 4 を付加した鍵生成用情報を生成する手段である。

なお、本実施の形態の鍵生成用情報は本発明の第 1 の情報の例である。

暗号器 5 5 は、鍵生成用情報を記録ユニット番号 2 5 を用いて暗号化したものであるコンテンツキーを生成する手段である。

暗号器 2 1 は、コンテンツ 2 6 をコンテンツキーを用いて暗号化する手段である。

図 1 4 に本実施の形態のハードディスク装置 2 の復号手段 6 3 を示す。

図 1 4 において、復号手段 1 3 は、加算器 5 6、復号器 5 7、復号器 3 3 から構成される。

加算器 5 6 は、秘密領域 1 8 に記憶されているデバイスユニークキー 1 3 を読み込み、デバイスユニークキー 1 3 の下位ビットに続けて C C I 3 6 を付加した鍵生成用情報を生成する手段である。

復号器 5 7 は、鍵生成用情報を記録ユニット番号 2 5 を用いて復号してコンテンツキーを生成する手段である。

復号器 3 3 は、暗号化されたコンテンツ 1 7 をコンテンツキーを用いて復号し

WO 01/48755

PCT/JP00/09260

70

、復号されたコンテンツ 37 を出力する手段である。

次に、このような本実施の形態の動作を第 1 の実施の形態との相違点である暗号化手段 62 と復号手段 63 の動作を中心に説明する。

まず、暗号化手段 62 の動作を説明する。

加算器 54 は、秘密領域 18 に記憶されているデバイスユニークキー 13 を読み込む。そして、デバイスユニークキー 13 の下位ビットに続けて CCI 24 を付加した鍵生成用情報を生成する。

さらに、暗号化手段 62 は、AV データに付加されて送られてきた CCI 24 を検出する。検出された CCI 24 は、制御手段 14 の制御に従って、記録手段 15 の磁気ディスク媒体 29 に CCI 27 として記録される。

そして、加算器 54 は、デバイスユニークキー 13 の下位ビットに続けて CCI 24 を付加した鍵生成用情報を生成する。

暗号化手段 62 は、記録する記録ユニットの記録ユニット番号 25 を求める。

暗号器 55 は、AV データを記録しようとしている記録ユニットの記録ユニット番号 25 を用いて、鍵生成用情報を暗号化する。この暗号化した情報のことをコンテンツキーと呼ぶことにする。コンテンツキーは、記録ユニット番号 25 で暗号化したので、記録ユニット毎に変化する。

次に、暗号器 21 は、これから記録する AV データであるコンテンツ 26 をコンテンツキーで暗号化する。

暗号化された AV データは、制御手段 14 の制御に従って、記録手段 15 の磁気ディスク媒体 29 の記録すべき記録ユニットに暗号化されたコンテンツ 17 として、記録される。

以下、同様に、鍵生成用情報を、記録ユニット毎に、記録ユニット番号 25 で

WO 01/48755

PCT/JP00/09260

71

暗号化してコンテンツキーを生成し、生成したコンテンツキーでコンテンツ 26 を暗号化し、暗号化したコンテンツ 17 を磁気ディスク媒体 29 に記録するという動作を繰り返す。

このようにして、ハードディスク媒体 29 は、著作権保護の必要な AV データを磁気ディスク媒体 29 に記録する。

次に、復号手段 63 の動作を説明する。

加算器 56 は、秘密領域 18 に記憶されているデバイスユニークキー 13 を読み込む。

制御手段 14 の制御に従って、記録手段 15 は、磁気ディスク媒体 29 から CCI 27 を読み出す。

復号手段 63 は、CCI 27 を I/F 4 に転送する。

加算器 56 は、デバイスユニークキー 13 の下位ビットに続けて CCI 27 を付加した鍵生成用情報を作成する。

制御手段 14 は、読み取るべき記録ユニット 39 を指定して、記録手段 15 が記録ユニット 39 に格納されている情報である暗号化されたコンテンツ 17 を読み取りよう制御する。

復号手段 63 は、記録ユニット 39 の記録ユニット番号 25 を求める。

復号器 57 は、データを読み出そうとしている記録ユニット 39 の記録ユニット番号 25 を用いて、鍵生成用情報を復号する。この復号した情報のことをコンテンツキーと呼ぶことにする。コンテンツキーは、記録ユニット番号 25 で復号したので、記録ユニット毎に変化する。

次に、制御手段 14 の制御に従って、記録手段 15 は、磁気ディスク媒体 29 の読み出すべき記録ユニットに格納されている情報である暗号化されたコンテ

WO 01/48755

PCT/JP00/09260

72

ツ 1 7 を読み出す。

次に、復号器 3 3 は、記録手段 1 5 が読み出した暗号化されたコンテンツ 1 7 をコンテンツキーで復号する。

復号手段 6 3 は、復号されたコンテンツ 3 7 を I / F 4 に転送する。

以下、同様に、鍵生成用情報を、記録ユニット毎に、記録ユニット番号 2 5 で復号してコンテンツキーを生成し、暗号化されたコンテンツ 1 7 を読み出し、暗号化されたコンテンツ 1 7 を、コンテンツキーで復号し、復号したコンテンツ 2 7 を M P E G 2 トランスポートストリームとして I / F 4 に転送するという動作を繰り返す。

本実施の形態で説明した暗号化手段 6 2 と復号手段 6 3 をハードディスク装置 2 に用いることにより、第 1 の実施の形態と同等の効果が得られる。

また、暗号化手段 6 2 と復号手段 6 3 を第 1 の実施の形態で説明した種々の変形例に適用出来ることは言うまでもない。

(第 6 の実施の形態)

次に、第 6 の実施の形態について説明する。

図 1 に、本発明の記録装置及び再生装置の一実施の形態であるハードディスク装置 2 を示す。本実施の形態のハードディスク装置 2 は、第 1 の実施の形態で説明したハードディスク装置 2 の暗号化手段 1 1 と復号手段 1 2 の代わりに別の暗号化手段と復号手段に置き換えたものである。

図 1 5 に本実施の形態のハードディスク装置 2 の暗号化手段 6 4 を示す。また、図 1 6 に本実施の形態の復号手段 6 5 を示す。

本実施の形態では、第 1 の実施の形態との相違点である暗号化手段 6 4 と復号手段 6 5 を中心に説明する。

WO 01/48755

PCT/JP00/09260

73

図15において、暗号化手段64は、暗号器58、暗号器21から構成される。本実施の形態の暗号化手段64は、暗号化手段11とは異なり、AVデータの暗号化にタイトルキーとCCIを用いない。

すなわち、暗号器58は、デバイスユニークキー13を記録ユニット番号25を用いて暗号化したものであるコンテンツキーを生成する手段である。

なお、本実施の形態のデバイスユニークキー13は本発明の第1の情報の例である。

暗号器21は、コンテンツ26をコンテンツキーを用いて暗号化する手段である。

図16に本実施の形態のハードディスク装置2の復号手段65を示す。

図16において、復号手段65は、復号器59、復号器33から構成される。

復号器59は、記録ユニット番号25を用いてデバイスユニークキー13を復号してコンテンツキーを生成する手段である。

復号器33は、暗号化されたコンテンツ17をコンテンツキーを用いて復号し、復号されたコンテンツ37を出力する手段である。

次に、このような本実施の形態の動作を第1の実施の形態との相違点である暗号化手段64と復号手段65の動作を中心に説明する。

まず、暗号化手段64の動作を説明する。

暗号化手段64は、AVデータに付加されて送られてきたCCI24を検出する。検出されたCCI24は、制御手段14の制御に従って、記録手段15の磁気ディスク媒体29にCCI27として記録される。

暗号器58は、デバイスユニークキー13を秘密領域18から読み取る。

暗号化手段64は、記録する記録ユニットの記録ユニット番号25を求める。

WO 01/48755

PCT/JP00/09260

74

暗号器 58 は、AV データを記録しようとしている記録ユニットの記録ユニット番号 25 を用いて、ディスクユニークキー 13 を暗号化する。この暗号化した情報のことをコンテンツキーと呼ぶことにする。コンテンツキーは、記録ユニット番号 25 で暗号化したので、記録ユニット毎に変化する。

次に、暗号器 21 は、これから記録する AV データであるコンテンツ 26 をコンテンツキーで暗号化する。

暗号化された AV データは、制御手段 14 の制御に従って、記録手段 15 の磁気ディスク媒体 29 の記録すべき記録ユニットに暗号化されたコンテンツ 17 として、記録される。

以下、同様に、デバイスユニークキー 13 を記録ユニット毎に、記録ユニット番号 25 で暗号化してコンテンツキーを生成し、生成したコンテンツキーでコンテンツ 26 を暗号化し、暗号化したコンテンツ 17 を磁気ディスク媒体 29 に記録するという動作を繰り返す。

このようにして、磁気ディスク媒体 29 には、著作権保護の必要な AV データが記録される。

次に、復号手段 63 の動作を説明する。

復号器 59 は、秘密領域 18 に記憶されているデバイスユニークキー 13 を読み込む。

制御手段 14 の制御に従って、記録手段 15 は、磁気ディスク媒体 29 から CCI 27 を読み出す。

復号手段 65 は、CCI 27 を I/F 4 に転送する。

制御手段 14 は、読み取るべき記録ユニット 39 を指定して、記録手段 15 が記録ユニット 39 に格納されている情報である暗号化されたコンテンツ 17 を読

WO 01/48755

PCT/JP00/09260

75

み取りよう制御する。

復号手段63は、記録ユニット39の記録ユニット番号25を求める。

復号器59は、データを読み出そうとしている記録ユニット39の記録ユニット番号25を用いて、デバイスユニークキーを復号する。この復号した情報のことをコンテンツキーと呼ぶことにする。コンテンツキーは、記録ユニット番号25で復号したので、記録ユニット毎に変化する。

次に、制御手段14の制御に従って、記録手段15は、磁気ディスク媒体29の読み出すべき記録ユニットに格納されている情報である暗号化されたコンテンツ17を読み出す。

次に、復号器33は、記録手段15が読み出した暗号化されたコンテンツ17をコンテンツキーで復号する。

復号手段63は、復号されたコンテンツ37をI/F4に転送する。

以下、同様に、デバイスユニークキー13を、記録ユニット毎に、記録ユニット番号25で復号してコンテンツキーを生成し、暗号化されたコンテンツ17を読み出し、暗号化されたコンテンツ17を、コンテンツキーで復号し、復号したコンテンツ27をMPEG2トランスポートストリームとしてI/F4に転送するという動作を繰り返す。

このように、復号手段65は、暗号化されたコンテンツ17を復号する。

本実施の形態で説明した暗号化手段64と復号手段65をハードディスク装置2に用いることにより、第1の実施の形態と同等の効果が得られる。

また、暗号化手段64と復号手段65を第1の実施の形態で説明した種々の変形例に適用出来ることは言うまでもない。

なお、第4～6の実施の形態で、種々の暗号化手段と復号手段を示したが、こ

WO 01/48755

PCT/JP00/09260

76

れに限らず、例えば図17、図18、図19に示すようなものもハードディスク装置2の暗号化手段11及び復号手段12の代わりに用いることが出来る。

図17の(a)に暗号化手段73を示す。暗号化手段73は、デバイスユニークキー13を用いて暗号器67がコンテンツ26を暗号化するものである。

また、図17の(b)に復号手段74を示す。復号手段74は、暗号化手段73によって暗号化されたコンテンツ17を複合器68がデバイスユニークキー13を用いて復号し、復号されたコンテンツ37を出力するものである。

図18の(a)に、暗号化手段75を示す。暗号化手段75は、記録ユニット番号25を用いて、暗号器69がコンテンツ26を暗号化するものである。

図18の(b)に、復号手段76を示す。復号手段76は、復号器70が暗号化手段75によって暗号化された暗号化されたコンテンツ17を、記録ユニット番号25を用いて復号し、復号されたコンテンツ37を出力するものである。

図19の(a)に、暗号化手段77を示す。暗号化手段77は、暗号器71がデバイスユニークキー13と記録ユニット番号25を用いてコンテンツ26を暗号化するものである。なお、暗号化手段77に加算器を追加し、加算器がデバイスユニークキー13と記録ユニット番号25を結合し、その情報を用いて、暗号器71がコンテンツ26を暗号化する構成にすることもできる。

図19の(b)に、復号手段78を示す。復号手段78は、暗号化手段77によって暗号化された暗号化されたコンテンツ17を、復号器72がデバイスユニークキー13と記録ユニット番号25を用いて復号するものである。

なお、復号手段78に加算器を追加し、加算器がデバイスユニークキーと記録ユニット番号25を結合し、その情報を用いて、復号器72が暗号化されたコンテンツ17を復号する構成でも構わない。

WO 01/48755

PCT/JP00/09260

77

(第7の実施の形態)

次に、第7の実施の形態について説明する。

図20の本発明の記録装置及び再生装置の一実施の形態であるハードディスク装置83の構成を示す。

ハードディスク装置83は、第1の実施の形態のハードディスク装置2に加えてCCI判定手段79、再生情報管理手段80を備えている。また、第1の実施の形態のI/F4の代わりにI/F81を、第1の実施の形態の制御手段14の代わりに制御手段82を備えている。

I/F81の第1の実施の形態のI/F4との相違点は、IEEE1394バス1から受け取ったAVデータのCCIがCopy Neverであっても、コントローラ10に記録処理を開始するように通知し、コントローラ10は、I/F81からの通知に従って、AVデータのCCIがCopy Neverであっても所定の条件のもとではそのAVデータを記録することが出来る点である。

またCCI判定手段79は、再生されたAVデータのCCIの値を判定し、再生後のCCIの値を決める手段である。

再生情報管理手段80は、記録手段15に記録されているAVデータを記録ユニット毎に一度再生されたかあるいは一度も再生されていないかの情報である再生情報を管理する手段である。

また、再生管理手段80は、記録手段15に記録されているAVデータが記録ユニット毎に他の機器に複製されたかまだ一度も複製されていないかを管理する手段でもある。

再生情報を参照すれば、記録ユニットに記録されているAVデータが1回再生済みであるかあるいは一度も再生されていないかを知ることが出来、例えば再生

WO 01/48755

PCT/JP00/09260

78

情報は1ビットのフラグで表すことが出来る。

また、複製情報を参照すれば、記録ユニットに記録されているAVデータが1回複製されたかあるいはまだ一度も複製されていないかを知ることが出来る。

制御手段82は、第1の実施の形態の制御手段14に加えて、再生中のAVデータのCCIをCCI判定手段79に供給し、再生中のAVデータのCCIと再生情報管理手段80が生成更新している再生情報に従って、記録手段15がAVデータの再生を行うか行わないかを制御し、また、他の機器への複製中のAVデータのCCIをCCI判定手段79に供給し、複製中のAVデータのCCIと再生情報管理手段80が生成更新している複製情報に従って、記録手段15がAVデータの複製を行うか行わないかを制御する手段である。

なお、本実施の形態のCCI判定手段79、制御手段82、再生情報管理手段80は、本発明の制御手段の例であり、本実施の形態のI/F81は本発明のインターフェースの例である。

次に、このような本実施の形態の動作を第1の実施の形態との相違点を中心に説明する。

まず、記録時の動作を説明する。

ホストシステムからはAVデータが送られてきている。

I/F81は、そのAVデータのCCIがCopy neverの場合もコントローラ84に記録を開始するように通知する。

暗号化手段11は、AVデータを暗号化する。

制御手段82の制御に従って、記録手段15は、暗号化されたAVデータを磁気ディスク29に記録する。この際、第1の実施の形態と同様にCCIも記録する。

WO 01/48755

PCT/JP00/09260

79

ただし、制御手段82は、CCIがCopy neverの場合であっても、そのAVデータを記録する。しかし記録手段15に記録されたCCIがcopy neverのAVデータは、記録されてから所定の時間後に再生不可となる。どのようにして所定の時間後に再生不可となるかについては、後述する。

また、制御手段82は、CCIがcopy onceのAVデータを複製するために出力するが、複製出力されてから所定の時間後には再生不可となる。これについても後述する。

再生情報管理手段80は、記録ユニット毎にAVデータが記録手段15に記録されると、再生情報と複製情報を次のように生成する。

すなわち、新規にAVデータが記録された時、記録ユニット毎に再生情報を未再生に設定し、複製情報を未複製に設定する。さらに、AVデータが記録された時刻を記録する。

次に、このようにして記録されたAVデータを再生する場合の動作を説明する。

再生情報管理手段80は、これから再生する記録ユニットのAVデータの再生情報を参照し、制御手段82に通知する。

さらに、CCI判定手段79は、これから再生するAVデータのCCIの値を判定し、再生出力される場合のCCIの値を決定する。

すなわち、再生されたAVデータのCCIがCopy neverの場合、I/F81から出力する際のCCIをCopy neverとする。また、再生されたAVデータのCCIがCopy onceの場合、I/F81から出力する際のCCIをNo more copyに変更する。また、CCIがCopy freeの場合、I/F81から出力する際のCCIをCopy freeとする。またCCIの値がNo more copyであるAVデータは記録されな

WO 01/48755

PCT/JP00/09260

80

いので、CCIがNo more copyとなることはない。

制御手段82の制御に従って、記録手段がAVデータを再生する。

再生情報管理手段80は、再生管理情報を次のように更新する。

すなわち、記録ユニット分のAVデータが再生されると、その再生情報を制御手段82に通知する。また、記録ユニット分のAVデータが再生されるとその部分の再生情報を再生済みに設定する。

再生情報管理手段80は、現在再生中のAVデータの再生情報がすでに再生済みであった場合、制御手段82に通知する。

また、再生情報管理手段80は、現在再生中のAVデータの時刻情報を制御手段82に通知する。

制御手段82は、CCI判定手段79によって変更される前のCCIの値に応じて以下の動作をする。

すなわち、CCIがCopy neverのAVデータであれば、再生情報が再生済みの部分の再生を中止するように制御する。また、再生情報管理手段80から通知された、そのAVデータに関する時刻情報が示す時刻から現在の時刻が所定の時間例えば240時間（10日間）以上経過している場合、そのAVデータを再生しないよう制御する。

また、CCIがCopy onceのAVデータの場合は、再生情報の値に関わらず再生を継続するように制御する。

また、CCIがCopy freeのAVデータの場合は再生を継続するよう制御する。

このようにして再生されたAVデータは復号手段12で復号される。

そして、I/F81で伝送用に暗号化されてIEEE1394バス1にアイン

WO 01/48755

PCT/JP00/09260

81

クロナスパケットとして出力される。この際アイソクロナスヘッダには、上記のようにCCI判定手段79が決めたCCIが付加されている。

次に、このようにして記録されたAVデータを複製する場合の動作を説明する。

再生情報管理手段80は、これから複製する記録ユニットのAVデータの複製情報を参照し、制御手段82に通知する。

さらに、CCI判定手段79は、これから複製するAVデータのCCIの値を判定し、再生出力される場合のCCIの値を決定する。

すなわち、再生されたAVデータのCCIがCopy neverの場合、I/F81から出力する際のCCIを設定しないかまたはCopy neverとする。また、再生されたAVデータのCCIがCopy onceの場合、I/F81から出力する際のCCIをCopy onceのままにし、No more copyに変更しない。また、CCIがCopy freeの場合、I/F81から出力する際のCCIをCopy freeとする。またCCIの値がNo more copyであるAVデータは記録されないので、CCIがNo more copyとなることは、ない。

制御手段82の制御に従って、記録手段が複製されるAVデータを再生する。

再生情報管理手段80は、複製管理情報を次のように更新する。

すなわち、記録ユニット分のAVデータが複製されると、その複製情報を制御手段82に通知する。また、記録ユニット分のAVデータが複製されるとその部分の複製情報を複製済みに設定する。

再生情報管理手段80は、現在複製中のAVデータの複製情報がすでに複製済みであった場合、制御手段82に通知する。

制御手段82は、CCI判定手段79によって変更される前のCCIの値に応

WO 01/48755

PCT/JP00/09260

82

じて以下の動作をする。

すなわち、CCIがCopy neverのAVデータであれば、複製をおこなわないように制御する。

また、CCIがCopy onceのAVデータの場合は、複製情報が複製済みの部分の複製を行わないよう制御し、複製情報が未複製の場合は、その部分のAVデータの記録先の装置がバックアップ用として前記データを記録する装置である場合に限り、複製を継続するよう制御する。

また、CCIがCopy freeのAVデータの場合は複製を継続するよう制御する。

このようにして複製されるために再生されたAVデータは復号手段12で復号される。

そして、I/F81で伝送用に暗号化されてIEEE1394バス1にアイソクロナスパケットとして出力される。この際アイソクロナスヘッダには、上記のようにCCI判定手段79が決めたCCIが付加されている。IEEE1394バス1を経由して他の機器で受信されて、記録される。

また、複製されたAVデータのCCIがcopy onceの場合、バックアップ用として記録された記録先ではそのAVデータを再生することが出来ず、元のハードディスク83に戻さないと再生出来ない。

すなわち、本実施の形態のハードディスク装置83は、Copy neverのAVデータを記録し、一回だけ再生することが出来る。

CCIがCopy neverのAVデータは記録することが許されていないので、放送される時間帯にのみ視聴するものであった。

しかし、本実施の形態のハードディスク装置83を用いれば、著作権者の意図

WO 01/48755

PCT/JP00/09260

83

を守ったまま、AVデータを放送される時間帯とは別の時間帯に視聴することが出来る。

また、CCIがCopy onceのAVデータは一回だけコピーすることが許可されるものであった。すなわち、一度、Copy onceのAVデータを記録すると、記録した装置からそのAVデータを再生することしか出来なかった。

しかし、本実施の形態のハードディスク装置83を用いれば、Copy onceのAVデータをCopy onceのCCIのまま一回だけ複製することが出来るので、著作権の意図するところを守ったままそのAVデータを別の記録再生装置に移動することが出来る。

なお、本実施の形態では、再生情報管理手段80が、記録ユニット分のAVデータが再生されると、その再生情報を制御手段82に通知し、記録ユニット分のAVデータが再生されるとその部分の再生情報を再生済みに設定することにより、本実施の形態のハードディスク装置83は、CCIがCopy neverのAVデータを1回だけ再生することが出来るとして説明したが、これに限らない。再生情報管理手段80が再生情報を更新する方法を以下のようにしても構わない。

すなわち、再生情報管理手段80が、記録ユニット分のAVデータが何回再生されたかをカウントし、所定の回数例えば5回だけ再生されてはじめてその記録ユニット分のAVデータの再生情報を再生済みに設定しても構わない。このようにすれば、ハードディスク装置83は、CCIがCopy neverのAVデータを所定の回数だけ再生することが出来るようになる。

また、再生情報管理手段80が、一つのAVデータのうちの各記録ユニットに記録されている部分が再生されたか回数をカウントし、一つのAVデータの全て

WO 01/48755

PCT/JP00/09260

84

の記録ユニットに記録されている部分が全て再生された時点で、再生情報管理手段 80 がこの一つの AV データの全ての記録ユニットに記録されている部分の再生管理情報を再生済みに設定しても構わない。このようにすれば、ハードディスク装置 83 は、CCI が Copy never の AV データの一部を何回でも再生することが出来るようになり、その AV データの全部が再生された時点ではじめて再生不可になる。

さらに、本実施の形態では、CCI が Copy never の AV データは記録されてから所定の時間が経過すると再生不可となるとして説明したが、これに限らず、CCI が Copy never の AV データが課金条件によって再生不可ととも構わない。このような課金条件としては、CCI が Copy never の AV データを記録したときに所定の代金の支払い手続きを行った場合には再生可として、その支払い手付きを行わなかった場合には再生不可となるなどの条件がある。

さらに、本実施の形態では、CCI が copy once の AV データは、複製情報が未複製の場合は、その部分の AV データの記録先の装置がバックアップ用として前記データを記録する装置である場合に限り、複製を継続するよう制御するとして説明したが、これに限らず、CCI が copy once の AV データを記録してから所定の時間が経過するとその記録された AV データまたはそのデータを記録する際の暗号化に用いたキーを消去しても構わない。

このように、本実施の形態のハードディスク装置 83 は、CCI が copy never の AV データを記録したり、CCI が Copy once の AV データを Copy once の CCI のまま一回だけ再生したりするので、

WO 01/48755

PCT/JP00/09260

85

著作権者の意図するところを守っているとは言え、著作権違反をしているとも捉えることが出来る。すなわち、CCIがcopy neverである場合には、絶対複製をしてはいけないという意味があるからである。ところで、このようなCCIの意味を拡張した拡張CCIの使用が現在検討中である。拡張CCIではcopy neverやcopy onceの意味を拡張して解釈される。本実施の形態のハードディスク装置83は、このような従来のCCIの代わりに拡張CCIを用いて上記のような動作を行うことも出来る。このように本実施の形態のハードディスク装置83が拡張CCIを用いて上記のような動作を行えば、著作権違反を犯していることにはならなくなる。

このように、本実施の形態のハードディスク装置83を用いれば、記録することが許されていないAVデータが放送される時間帯以外の任意の時間に視聴することが出来る。また、1世代しか複製を作ることが許されていないAVデータを別の記録装置に移動することが出来るのでバックアップ装置としても使用することが出来る。

なお、記録することが許されていないAVデータを放送される時間帯以外の任意の時間帯に視聴したり、バックアップすることについては、以下の実施の形態でさらに、詳細に説明する。

なお、本実施の形態のハードディスク装置83にも、第1の実施の形態で説明した種々の変形が可能であることは言うまでもない。

さらに、本実施の形態のハードディスク装置83は、暗号化手段11、復号手段12を備えているとして説明したが、第1の実施の形態以降で説明した暗号化手段、復号手段を用いても構わない。

さらに、本発明のデータは、本実施の形態におけるAVデータに限らない。イ

WO 01/48755

PCT/JP00/09260

86

インターネットなどから送られてくる文書データや画像データ、インターネットなどから送られてくるゲームソフトや文書作成ソフトなどのコンピュータプログラムであっても構わない。要するに本発明のデータとは、本発明のディスクに記録し、本発明のディスクから再生して利用することが出来るものでありさえすればよい。

さらに、本発明のインターフェースは、本実施の形態におけるIEEE 1394インターフェースに限らず、USBのインターフェースであっても構わない。

さらに、本発明のディスクは、本実施の形態における磁気ディスク媒体に限らず、光ディスク媒体や光磁気ディスク媒体などであっても構わない。要するに本発明のディスクは、記録時及び／または再生時にデータにランダムアクセスすることが出来る記録媒体でありさえすればよい。

さらに、本発明のコピー許諾情報は、本実施の形態におけるCCIや拡張CCIなどに限らず、要するにデータを複製することに関する許諾を示す情報でありさえすればよい。

なお、以上の実施の形態では、AVデータに付加されているCCIの値として、Copy never、Copy once、No more copy、Copy freeがあるとして説明したが、以下に説明する第8～第11の実施の形態では、CCIの値がCopy Never、Copy once、及びNo more CopyのいずれかであるAVデータは、コピー禁止データとして一括して扱うものとする。また、コピー禁止データのCCIが上記のCopy Never、Copy once、及びNo more Copyのいずれに対応しているかについては、第8～第11の実施の形態で個別に説明するものとする。

WO 01/48755

PCT/JP00/09260

87

(第8の実施の形態)

次に、本発明の第8の実施の形態のAVHDD1001およびアーカイブ機器1002の構成を述べる。

図21に、本発明の第8の実施の形態のAVHDD1001およびアーカイブ機器1002のブロック図を示す。なお、図21には説明の便宜上、STB(セットトップボックス)1003をも表示している。

さて、本発明の第8の実施の形態のAVHDD1001は、図21に示すように、STB1003からのデータをAVHDD1001固有の暗号化鍵で暗号化する暗号化手段1004と、暗号化手段1004によって暗号化されたデータを蓄積手段1006内の記録媒体に記録する第1記録手段1005と、データを蓄積する蓄積手段1006と、蓄積手段1006に蓄積されているデータをアーカイブ機器1002に移動させる移動手段1007と、アーカイブ機器1002からのデータであって、AVHDD1001固有の暗号化鍵で暗号化されているデータを解読し再生する再生手段8とで構成されている。なお、蓄積手段1006は、データが記録される第1の記録媒体を有しており、データはその第1の記録媒体に記録される。

なお「発明の実施の形態」では、AVHDDを、ハードディスクドライブ(HDD)を用いて、音声(Audio)や映像(Video)やその他のデータを記録再生する装置を表す単語として用いる。

次に、本発明の第8の実施の形態のアーカイブ機器1002は、図21に示すように、AVHDD1001からのデータを第2の記録媒体1010に記録する第2記録手段1009と、第2の記録媒体1010と、第2の記録媒体1010に記録されているデータを読み出してAVHDD1001に送

WO 01/48755

PCT/JP00/09260

88

信する送信手段1011とで構成されている。なお、アーカイブ機器1002としては、例えばDVD装置や、D-VHS装置が該当する。本実施の形態では、アーカイブ機器1002の一例としてDVD装置を用いて説明することにする。したがって、第2の記録媒体1010の一例としてはDVDが該当することになる。

なお、STB1003は、例えば放送局からのデータを受信し、そのデータをAVHDD1001に出力するとともに、AVHDD1001からのデータを再生する手段であって、再生されたデータは、映像データであればSTB1003に接続されているディスプレイに表示され、また音声データであればSTB1003に接続されているスピーカから出力される。なお、ディスプレイやスピーカは図示されていない。

また、第8の実施の形態では、本発明の、データ処理装置の一例としてAVHDD1001を、記録再生装置の一例としてアーカイブ機器1002を、それぞれ用いる。

また、AVHDD1001の蓄積手段1006内の第1の記録媒体は、リムーバブルの記録媒体であってもよいし、固定設置型の記録媒体であってもよい。同様に、アーカイブ機器1002内の第2の記録媒体1010も、リムーバブルの記録媒体であってもよいし、固定設置型の記録媒体であってもよい。

また、AVHDD1001とアーカイブ機器1002との接続は、IEEE1394規格のインターフェースを介して行われていてもよいし、IDE規格のインターフェースを介して行われていてもよい。または、他のインターフェースを介して行われていてもよい。AVHDD1001とSTB10

WO 01/48755

PCT/JP00/09260

89

03との接続についても、いずれのインターフェースを介して行われていてもよい。

次に、本発明の第8の実施の形態のAVHDD1001およびアーカイブ機器1002の動作を述べる。

以下の説明の便宜上、AVHDD1001の蓄積手段1006内の第1の記録媒体の記録可能容量が限界に達しようとしており、いずれかのデータを上書きまたは削除しなければSTB1003からの新たなデータを蓄積することができない状態であるとし、ユーザが、蓄積手段1006内のデータをアーカイブ機器1002内の第2の記録媒体1010に移動させるための指示を、AVHDD1001およびアーカイブ機器1002にしたものとする。

なお、データの移動とは、例えば第1の記録媒体に記録されているデータを、別の第2の記録媒体に移し、移した後には第1の記録媒体内には移ったデータを残さないことを意味する。

また、以下の説明の便宜上、AVHDD1001からアーカイブ機器1002に移動させられるデータは、暗号化手段1004によってAVHDD1001固有の暗号化鍵で暗号化され、第1記録手段1005によって蓄積手段1006内の第1の記録媒体に記録されていたものとする。また、上記の移動対象のデータは、著作権保護のために、他の記録装置への移動は許されているがコピーが禁止されているコピー禁止データであるとする。

さてこのとき、移動手段1007は、AVHDD1001固有の暗号化鍵で暗号化されているコピー禁止データを、蓄積手段1006内の第1の記録媒体から読み出してアーカイブ機器1002に送信する。このようにして移動手段1007がコピー禁止データを送信するさい（移動させるさい）、そ

WO 01/48755

PCT/JP00/09260

90

の移動手段1007は、コピー禁止データを1回だけコピー可能なデータとして出力する。

そして、アーカイブ機器1002では、第2記録手段1009が、AVHDD1001からのコピー禁止データを第2の記録媒体1010に記録する。なお、移動手段1007によってアーカイブ機器1002に移動させられるデータは、AVHDD1001内において復号されずに暗号化されたままアーカイブ機器1002に移動させられる。したがって、第2記録手段1009によって第2の記録媒体1010に記録されたデータは、AVHDD1001固有の暗号化鍵で暗号化されているコピー禁止データであるということになる。

次に、第2の記録媒体1010に記録された、暗号化されているコピー禁止データを再生する場合について説明する。図21に示すように、アーカイブ機器1002には、暗号化されたコピー禁止データを解読し再生する手段が設けられていないので、コピー禁止データを解読し再生することができる、AVHDD1001の再生手段1008に再度データを移動させる必要がある。

そこで、第2の記録媒体1010に記録された、暗号化されているコピー禁止データを再生する場合には、送信手段1011が、第2の記録媒体1010に記録されているデータを読み出してAVHDD1001に送信し、AVHDD1001において、再生手段1008が、暗号化されたコピー禁止データを解読し再生する。

その解読され再生されたデータは、STB1003に出力され、映像データであればSTB1003に接続されているディスプレイに表示され、音声

WO 01/48755

PCT/JP00/09260

91

データであればSTB1003に接続されているディスプレイから出力される。

このように、例えばAVHDD1001の蓄積手段1006内の第1の記録媒体の記録可能容量が限界に達しようとしている場合であっても、蓄積手段1006内のデータを上書きするなどして削除せずに、他の記録媒体にデータを移動させることができるので、後に移動させたデータを再生することができるというメリットがある。

また、不正行為によって、アーカイブ機器1002に対応する、第2の記録媒体1010と同様のメディアが大量に複製され、そして配布されたとしても、そのメディアに記録されているデータは、AVHDD1001の暗号化手段1004によって、AVHDD1001固有の暗号化鍵で暗号化されたデータであるので、そのデータを再生することができるのはAVHDD1001のみであり、著作権保護の対象データであるコピー禁止データを、著作権を保護して他の装置、つまりアーカイブ機器1002に移動させることができる。したがって、安全なデータの移動を実現できるということである。なお、生産された複数のAVHDD1001の固有の暗号化鍵は、それぞれ異なる。

なお、上述した実施の形態では、コピー禁止データは、AVHDD1001の暗号化手段1004によって、AVHDD1001固有の暗号化鍵で暗号化されるとしたが、コピー禁止データは、暗号化手段1004によって暗号化されるものと限定することはない。例えば、AVHDD1001の製造段階で、AVHDD1001固有の暗号化鍵で暗号化されたコピー禁止データが蓄積手段1006内の第1の記録媒体に記録されていてもよい。

WO 01/48755

PCT/JP00/09260

92

また、上述した実施の形態では、コピー禁止データは、暗号化手段1004によって暗号化された後に蓄積手段1006内の第1の記録媒体の記録されているとしたが、暗号化手段1004が蓄積手段1006と移動手段1007との間に設けられており、コピー禁止データが、移動手段1007によって移動させられるさいに、AVHDD1001固有の暗号化鍵で暗号化されるとしてもよい。要するに、移動手段1007が移動させようとするコピー禁止データは、少なくともAVHDD1001から出力するさいに、そのAVHDD1001固有の暗号化鍵で暗号化されておりさえすればよい。

また、本実施の形態では、コピー禁止データは、他の記録装置への移動は許されているがコピーが禁止されているデータであるとしたが、「発明の実施の形態」における「コピー禁止データ」には、2bitで「01」と表される「これ以上コピー禁止」というデータや、2bitで「11」と表される「絶対的にコピー禁止」というデータも含まれる。

また、図21を用いて説明した上記実施の形態の送信手段1011が、図23に示すような、第2の記録媒体1010に記録されているデータを通常のN倍速（Nは1を超える正数）でAVHDD1001に送信する高速送信手段1015に置き換えられていてもよい。その場合、図21のAVHDD1001を、データ格納手段としてのバッファ1014がさらに設けられているAVHDD1012に置き換えて、高速送信手段1015からのデータをバッファ1014に一時的に格納し、その一時的に格納されたデータを、再生手段1008に再生させることができる。

そうすると、アーカイブ機器1013からAVHDD1012にN倍速（高速）でデータ転送をするとともに、AVHDD1012においてデータを

WO 01/48755

PCT/JP00/09260

93

通常再生することができるというメリットがでてくる。なお、バッファ 1014 は、蓄積手段 1006 内に設けられていてもよい。また、「通常の N 倍速」とは、再生手段 1008 がデータを再生するさいの、ユーザが視聴するさいに必要なデータ再生速度よりも速い速度を意味する。

なお、図 23 を用いて説明した例では、アーカイブ機器 1013 に高速送信手段 1015 を設けて、アーカイブ機器 1013 から AVHDD 1012 に N 倍速（高速）でデータ転送するとしたが、AVHDD の移動手段 1007 を、N 倍速（N は 1 を超える正数）でデータをアーカイブ機器に高速移動させる高速移動手段に置き換えてもよい。その場合、アーカイブ機器にはデータを一時的に格納するバッファを設けておくことが好ましい。このように、AVHDD に高速移動手段を設けておくと、AVHDD からアーカイブ機器に短時間でデータ移動を行わせることができるというメリットがでてくる。また、後述する実施の形態 2 における AVHDD においても、移動手段の替わりに高速移動手段を設けると、短時間でデータ移動を行わせることができるという効果が現れる。

また、上述した実施の形態では、アーカイブ機器 1002 には、AVHDD 1001 固有の暗号化鍵で暗号化されているデータを解読し再生する手段は設けられていなかったが、図 23 に示すように、アーカイブ機器 1002 を、AVHDD 1001 固有の暗号化鍵で暗号化されているデータを解読し再生する解読再生手段 1017 を備えたアーカイブ機器 1016 に置き換えて、AVHDD 1001 にデータ送信することなく、アーカイブ機器 1016 において、AVHDD 1001 固有の暗号化鍵で暗号化されているデータを解読させ再生するとしてもよい。

WO 01/48755

PCT/JP00/09260

94

このように、アーカイブ機器1016においてAVHDD1001固有の暗号化鍵で暗号化されているデータを解読し再生することができると、データを再生するためにのみアーカイブ機器1002とAVHDD1001とを接続しなければならないという問題は解消される。

なお、アーカイブ機器1016の解読再生手段1017が、暗号化されているデータを解読し再生するには、AVHDD1001固有の暗号化鍵が必要となるが、アーカイブ機器1016にICカードスロットをあらかじめ設けておき、図23に示すように、AVHDD1001固有の暗号化鍵が記録されているICカード1018がICカードスロットに挿入された場合に、解読再生手段1017がICカード1018からAVHDD1001固有の暗号化鍵を取得し、その暗号化鍵を用いて暗号化されているデータを解読し再生するとしてもよい。

また、ICカード1018を用いる場合、解読再生手段1017とは別に、ICカード1018を再生する鍵再生手段をアーカイブ機器1016に設けてもよい。また、ICカード1018からのAVHDD1001固有の暗号化鍵を記憶する鍵記憶手段をアーカイブ機器1016に設けてもよい。このように、アーカイブ機器1016に鍵記憶手段が設けられていると、第2の記録媒体1010に記録されている、AVHDD1001固有の暗号化鍵で暗号化されているデータを解読し再生するさい、その都度ICカード1018がICカードスロットに挿入されなければならないという問題を回避することができる。なお、ICカード1018に記録されている鍵としては、鍵の漏洩を防止するために、秘密鍵と公開鍵とを組み合わせたものとすることができる。

WO 01/48755

PCT/JP00/09260

95

また、上記の記載では、解読再生手段1017は、直接的にまたは間接的にICカード1018からAVHDD1001固有の暗号化鍵を取得するとしたが、解読再生手段1017は、ICカード1018の替わりに、AVHDD1001固有の暗号化鍵が記録されているまたは埋め込まれているKEYディスクやKEYカセットから暗号化鍵を取得するとしてもよい。なお、第2の記録媒体1010に、AVHDD1001固有の暗号化鍵が記録されていてもよい。その場合、ICカード1018や、KEYディスクや、KEYカセットは必要なくなる。

また、ICカード1018、KEYディスクまたはKEYカセットを用いるのではなく、AVHDD1001に、AVHDD1001固有の暗号化鍵を送信する手段を設けておくとともに、アーカイブ機器1016に、AVHDD1001からの暗号化鍵を受信する手段を設けておいて、解読再生手段1017が、送信されてきた暗号化鍵を用いて、暗号化されているデータを解読し再生するとしてもよい。

また、上述した実施の形態では、図21に示したように、AVHDD1001は、アーカイブ機器1002に暗号化されたデータを無条件で移動するとしたが、図24に示すように、図21のアーカイブ機器2の第2の記録媒体1010を、AVHDD1019に対応する記録媒体であることを示す認証情報が記録されている第2の記録媒体1021に置き換え、それと同時にAVHDD1001を、第2の記録媒体1021がAVHDD1019に対応する記録媒体であるか否かを判断する判断手段1020を備えたAVHDD1019に置き換えて、判断手段1020によって、第2の記録媒体1021がAVHDD1019に対応する記録媒体であると判断された場合に限

WO 01/48755

PCT/JP00/09260

96

り、移動手段1007が、AVHDD1019からアーカイブ機器1002にデータを移動させるとしてもよい。

なお、判断手段1020は、第2の記録媒体1021に認証情報が記録されていれば、第2の記録媒体1021がAVHDD1019に対応する記録媒体であるものと判断し、認証情報が記録されていないければ、第2の記録媒体1021がAVHDD1019に対応しないものと判断する。

ところで、認証情報が記録されている第2の記録媒体1021は、認証情報が記録されていない記録媒体と区別するために、認証情報が記録されていない記録媒体の表面の色とは異なる色を表面に有するディスクであるとしてもよく、また、著作権保護用の記録媒体であるので、認証情報が記録されていない記録媒体よりも所定の額だけ高価にしてもよい。そして、認証情報が記録されていない記録媒体の価格との差額の全部または一部が、著作権者または著作権団体に還元されるとしてもよい。

なお、第2の記録媒体1021がAVHDD1019に対応する記録媒体である場合にAVHDD1019からアーカイブ機器1002にデータが移動されるのではなく、アーカイブ機器1002がAVHDD1019に対応する装置である場合にAVHDD1019からアーカイブ機器1002にデータが移動されるとしてもよい。その場合、AVHDD1019には、アーカイブ機器1002がAVHDD1019に対応する装置であるか否かを判断する判断手段が設けられることになる。

また、AVHDD1001とアーカイブ機器2とが接続されたインタフェースに、少なくともコピー禁止データの移動に対して課金能力を有する管理装置が接続されていることが確認されたときに、AVHDD1001の移動

手段1007は、そのコピー禁止データをアーカイブ機器2に移動させるとしてもよい。なお、管理装置の一例としてはSTBが挙げられる。

また、上述した実施の形態では、AVHDDからアーカイブ機器にコピー禁止データを移動させるとした。つまり、コピー禁止データをアーカイブ機器に移動させた後にはAVHDDからコピー禁止データを削除するとした。しかしながら、アーカイブ機器においてコピー禁止データが処理できなくなることも考えられるので、コピー禁止データをAVHDDにバックアップとして残しておくことが好ましい場合がある。

その場合、上述した実施の形態の各AVHDDの移動手段1007を、コピー禁止データをアーカイブ機器にコピーする複写手段に置き換えると、アーカイブ機器にコピー禁止データを送信するとともに、AVHDD内にコピー禁止データをバックアップ蓄積しておくことができ、アーカイブ機器においてコピー禁止データが処理できなくなった場合でも、AVHDDにバックアップ蓄積されたコピー禁止データを利用することができるというメリットが生まれる。

ここで、複写手段を備えたAVHDDの構成の一例として、図21に示す移動手段1007を備えたAVHDD1001を、移動手段1007の替わりに複写手段1080を備えたAVHDD1081に置き換えた場合を例にとって、図28に示す。

(第9の実施の形態)

次に、本発明の第9の実施の形態のAVHDD1022およびアーカイブ機器1023の構成を述べる。

図25に、本発明の第9の実施の形態のAVHDD1022およびアーカ

WO 01/48755

PCT/JP00/09260

98

イブ機器 1023 のブロック図を示す。なお、上記第 8 の実施の形態の図 21 と同様に、説明の便宜上、図 25 には STB 1003 も表示している。

さて、本発明の第 9 の実施の形態の AVHDD 1022 は、図 25 に示すように、STB 1003 からのデータを蓄積手段 1025 内の記録媒体に記録する第 3 記録手段 1024 と、データを蓄積する蓄積手段 1025 と、蓄積手段 1025 に蓄積されているデータを平文化する平文化手段 1026 と、平文化手段 1026 によって平文化された、蓄積手段 1025 に蓄積されていたデータをアーカイブ機器 1023 に移動させる移動手段 1027 とで構成されている。

本発明の第 9 の実施の形態のアーカイブ機器 1023 は、図 25 に示すように、AVHDD 1022 からのデータをアーカイブ機器 1023 固有の暗号化鍵を用いて暗号化する暗号化手段 1028 と、暗号化手段 1028 によって暗号化されたデータを第 3 の記録媒体 1030 に記録する第 4 記録手段 1029 と、第 3 の記録媒体 1030 と、第 3 の記録媒体 1030 に記録されたデータをアーカイブ機器 1023 固有の暗号化鍵を用いて解読し再生する再生手段 1031 とで構成されている。なお、アーカイブ機器 1023 としては、例えば DVD 装置や、D-VHS 装置が該当する。本実施の形態では、アーカイブ機器 1023 の一例として DVD 装置を用い、第 3 の記録媒体 1030 の一例としては DVD を用いる。

また、第 9 の実施の形態では、本発明の、データ処理装置の一例として AVHDD 1022 を、記録再生装置の一例としてアーカイブ機器 1023 を、それぞれ用いる。

また、AVHDD 1022 の蓄積手段 1025 内の記録媒体は、リムーバ

WO 01/48755

PCT/JP00/09260

99

ブルの記録媒体であってもよいし、固定設置型の記録媒体であってもよい。同様に、アーカイブ機器 1023 内の第 3 の記録媒体 1030 も、リムーバブルの記録媒体であってもよいし、固定設置型の記録媒体であってもよい。

また、AVHDD 1022 とアーカイブ機器 1023 の接続は、図 21 を用いて説明した第 8 の実施の形態と同様に、いずれのインターフェースを介して行われていてもよい。

次に、本発明の第 9 の実施の形態の AVHDD 22 およびアーカイブ機器 23 の動作を述べる。

ユーザによって、蓄積手段 1025 内のデータをアーカイブ機器 1023 内の第 3 の記録媒体 1030 に移動させるための指示が、AVHDD 1022 およびアーカイブ機器 1023 に対してされたとする。なお、データの移動とは、第 8 の実施の形態で述べた通り、例えば第 1 の記録媒体に記録されているデータを、別の第 2 の記録媒体に移し、移した後には第 1 の記録媒体内には移ったデータを残さないことを意味する。

また、以下の説明の便宜上、移動対象のデータは、著作権保護のために、他の記録装置への移動は許されているがコピーが禁止されているコピー禁止データであって、第 3 記録手段 1024 によって蓄積手段 1025 内の記録媒体に記録されていたものであるとする。

さてこのとき、平文化手段 1026 は、蓄積手段 1025 に蓄積されているデータを平文化し、移動手段 1027 は平文のコピー禁止データを、蓄積手段 1025 内の記録媒体から読み出してアーカイブ機器 1023 に送信する。このようにして移動手段 1027 がコピー禁止データを送信するさい（移動させるさい）、その移動手段 1027 は、コピー禁止データを 1 回だけ

WO 01/48755

PCT/JP00/09260

100

コピー可能なデータとして出力する。

そして、アーカイブ機器 1023 では、暗号化手段 1028 が、AVHDD 1022 からのデータをアーカイブ機器 1023 固有の暗号化鍵を用いて暗号化し、第 4 記録手段 1029 が、暗号化手段 1028 によって暗号化されたデータを第 3 の記録媒体 1030 に記録する。なお、データは、アーカイブ機器 1023 に入力されたさい、もしくは第 3 の記録媒体 1030 に記録されたさいに、コピー禁止データとして扱われるものとする。

なお、AVHDD 1022 からアーカイブ機器 1023 へのデータの伝送経路上では、例えば D T C P で伝送データは保護されるとしてもよい。

次に、第 3 の記録媒体 1030 に記録された、アーカイブ機器 1023 固有の暗号化鍵で暗号化されているコピー禁止データを再生する場合について説明する。その場合、再生手段 1031 は、アーカイブ機器 1023 固有の暗号化鍵を用いて、第 3 の記録媒体 1030 に記録されたコピー禁止データを再生することになる。

このように、アーカイブ機器 1023 では、アーカイブ機器 1023 固有の暗号化鍵でデータを暗号化し記録するので、アーカイブ機器 1023 内で、記録したデータを再生することができるというメリットがある。

なお、上述した実施の形態では、アーカイブ機器 1023 の暗号化手段 1028 は、AVHDD 1022 からのコピー禁止データをアーカイブ機器 1023 固有の暗号化鍵を用いて暗号化するとしたが、第 3 の記録媒体 1030 に暗号化鍵が記録されている場合、暗号化手段 1028 は、第 3 の記録媒体 1030 に記録されている暗号化鍵を用いて、AVHDD 1022 からのコピー禁止データを暗号化するとしてもよい。この場合、再生手段 1031

WO 01/48755

PCT/JP00/09260

101

は、第3の記録媒体1030に記録されている暗号化鍵を用いて、コピー禁止データを再生することになる。

また、上述した実施の形態では、AVHDD1022からアーカイブ機器1023へ移動するデータは平文データであるとしたが、移動データは、アーカイブ機器1023固有の暗号化鍵で暗号化されたデータであってもよいし、第3の記録媒体1030に暗号化鍵が記録されている場合、その第3の記録媒体1030に記録されている暗号化鍵で暗号化されたデータであってもよい。

その場合、AVHDD1022には、アーカイブ機器1023固有の暗号化鍵を用いて、または第3の記録媒体1030に記録されている暗号化鍵を用いて、コピー禁止データを暗号化する暗号化手段が設けられることになる。また、AVHDD1022には、アーカイブ機器1023固有の暗号化鍵をアーカイブ機器1023から取得する手段や、第3の記録媒体1030に記録されている暗号化鍵をアーカイブ機器1023から取得する手段が設けられることになる。なお、アーカイブ機器1023からは、暗号化手段28が不要となる。

また、AVHDD1022からアーカイブ機器1023へ移動するデータは、アーカイブ機器1023において用いられるフォーマットのデータであってもよい。その場合、AVHDD1022には、移動させるデータをアーカイブ機器1023用のフォーマットのデータに変換するフォーマット変換手段が設けられるとすることができる。また、AVHDD1022において蓄積手段1025内にデータを記録するさい、そのデータは、アーカイブ機器1023において用いられるフォーマットで記録されるとしてもよい。

WO 01/48755

PCT/JP00/09260

102

また、第8の実施の形態において図24を用いて説明したように、AVHDD1022に、第3の記録媒体1030がAVHDD1022に対応する記録媒体であるか否かを判断する判断手段を設けて、その判断手段によって、第3の記録媒体1030がAVHDD1022に対応する記録媒体であると判断された場合に、移動手段1027は、平文のまたは暗号化されたコピー禁止データをアーカイブ機器1023に移動させるとしてもよい。

なお、第3の記録媒体1030に、その第3の記録媒体1030がAVHDD1022に対応する記録媒体であるかことを示す鍵が付されている場合、AVHDD1022に設けられる判断手段は、第3の記録媒体1030に付されている鍵を利用して、第3の記録媒体1030がAVHDD1022に対応する記録媒体であるか否かを判断するとしてもよい。

また、第3の記録媒体1030がAVHDD1022に対応する記録媒体であるか否かを判断してデータ移動を行うのではなく、アーカイブ機器1023がAVHDD1022に対応する装置であるか否かを判断してデータ移動を行ってもよい。その場合、AVHDD1022には、アーカイブ機器1023がAVHDD1022に対応する装置であるか否かを判断する判断手段が設けられることになり、その判断手段によって、アーカイブ機器1023がAVHDD1022に対応する装置であると判断された場合に、移動手段1027は、平文のまたは暗号化されたコピー禁止データをアーカイブ機器1023に移動させるとしてもよい。

なお、アーカイブ機器1023がAVHDD1022に対応する装置であるかことを示す鍵を有している場合、AVHDD1022に設けられる判断手段は、アーカイブ機器1023が有している鍵を利用して、アーカイブ機

WO 01/48755

PCT/JP00/09260

103

器 1 0 2 3 が AVHDD 1 0 2 2 に対応する装置であるか否かを判断するとしてもよい。

また、AVHDD 1 0 2 2 とアーカイブ機器 1 0 2 3 とが接続されたインタフェースに、少なくともコピー禁止データの移動に対して課金能力を有する管理装置が接続されていることが確認されたときに、AVHDD 1 0 2 2 の移動手段 1 0 2 7 は、そのコピー禁止データをアーカイブ機器 1 0 2 3 に移動させるとしてもよい。なお、管理装置の一例としては S T B が挙げられる。

また、第 8 の実施の形態および 2 の各 AVHDD には、データの移動を行ったさい、そのデータの移動に対する課金情報を、各 AVHDD を管理する管理装置に送信する手段が設けられていてもよい。また、管理装置の一例として、課金を行う手段が組み込まれている S T B 1 0 0 3 を用いることができる。

また、上述した実施の形態では、AVHDD からアーカイブ機器にコピー禁止データを移動させるとした。つまり、コピー禁止データをアーカイブ機器に移動させた後には AVHDD からコピー禁止データを削除するとした。しかしながら、アーカイブ機器においてコピー禁止データが処理できなくなることとも考えられるので、コピー禁止データを AVHDD にバックアップとして残しておくことが好ましい場合がある。

その場合、上述した実施の形態の AVHDD の移動手段 1 0 2 7 を、コピー禁止データをアーカイブ機器にコピーする複写手段に置き換えると、アーカイブ機器にコピー禁止データを送信するとともに、AVHDD 内にコピー禁止データをバックアップ蓄積しておくことができ、アーカイブ機器におい

WO 01/48755

PCT/JP00/09260

104

てコピー禁止データが処理できなくなった場合でも、AVHDDにバックアップ蓄積されたコピー禁止データを利用することができるというメリットが生まれる。

ここで、複写手段を備えたAVHDDの構成の一例として、図24に示す移動手段1007を備えたAVHDD1022を、移動手段1027の替わりに複写手段1090を備えたAVHDD1091に置き換えた場合を例にとって、図29に示す。

(第10の実施の形態)

次に、本発明の第10の実施の形態の暗号化データ復号記録システムについて説明する。

図30に、本第10の実施の形態の暗号化データ復号記録システムの構成を示す。図30に示すように、本第10の実施の形態の暗号化データ復号記録システムは、5個の記録装置1100a～1100eと、復号記録装置1101とで構成されている。

図31に本第10の実施の形態における各記録装置1100の構成を示す。図31に示すように、各記録装置1100は、記録手段1102と、その記録手段1102に記録されているデータを出力する出力手段1103とを有している。ここで、記録手段1102に記録されているデータは、コピーが禁止されているコピー禁止データが暗号化されたデータであって、各記録装置1100の記録手段1102には、同じ内容の暗号化されたコピー禁止データが記録されているものとする。

次に、図32に本第10の実施の形態における復号記録装置1101の構成を示す。図32に示すように、復号記録装置1101は、復号手段110

WO 01/48755

PCT/JP00/09260

105

4と、記録手段1105とを有している。ここで、復号手段1104は、記録装置1100から出力される暗号化されたコピー禁止データを復号する手段であって、記録手段1105は、記録装置1100に記録されているコピー禁止データと同じ内容のデータであって、暗号化されているコピー禁止データ、または暗号化されていないコピー禁止データを記録する手段である。

ところで、上述した本第10の実施の形態の暗号化データ復号記録システムでは、同じ内容のデータが、5個の記録装置1100a～1100e、および復号記録装置1101それぞれに記録されているが、暗号化されたコピー禁止データは、復号記録装置1101の復号手段1104でしか復号され得ない。

したがって、本第10の実施の形態の暗号化データ復号記録システムを用いると、著作権を保護しつつ、データをその著作権を保護すべきデータをバックアップしておくことができるという効果が現れる。

なお、上述した実施の形態における暗号化データ復号記録システムは、記録装置1100は、a～1100eを備えているとしたが、記録装置1100の個数は5個に限定されるものではない。要するに複数個存在しておりさえすればよい。

(第11の実施の形態)

次に、本発明の第11の実施の形態のAVHDD1032について説明する。なお第11の実施の形態では、AVHDD1032からのデータの送信について述べるが、その送信するデータはDVD装置1033のDVD1037に記録されるものとする。

図26に、本発明の第11の実施の形態のAVHDD1032およびDV

WO 01/48755

PCT/JP00/09260

106

D装置1033のブロック図を示す。

さて、本発明の第11の実施の形態のAVHDD1032は、図26に示すように、データを蓄積する蓄積手段1034と、蓄積手段1034に蓄積されているデータをDVD装置1033に送信する送信手段1035とで構成されている。

本発明の第11の実施の形態のDVD装置1033は、図26に示すように、AVHDD1032からのデータをDVD1037に記録する第5記録手段1036と、第5記録手段1036に記録されたデータを再生する再生手段1038とで構成されている。

なお、第11の実施の形態では、本発明の、データ送信装置の一例としてAVHDD1032を用いる。

また、AVHDD1032とDVD装置1033の接続は、どのようなインターフェースを介して行われていてもよい。

次に、本発明の第11の実施の形態のAVHDD1032およびDVD装置1033の動作を述べる。

ここで、AVHDD1032が送信するデータは、複数個のデータパケットで構成されているストリームであるとする。図27に、そのストリームの一部の構成を示す。ストリームは、図27に示すような、D0、D1、D2、D3、D4の5個のデータパケットで構成されるブロック複数個で構成されるストリームであって、D0、D1、D2、D3、D4それぞれは、数字が大きくなる順番で時間的に連続するデータパケットであって、時間上の一つ手前のデータが再生されないと再生されないようになっている、連鎖暗号化されたデータである。

したがって、データパケットD0、D1、D2を取り上げると、データパケットD0の時間的に後に続くものがデータパケットD1であって、その次に続くものがデータパケットD2ということになり、データパケットD1は、データパケットD0が再生されないで再生されず、データパケットD2は、データパケットD1が再生されないで再生されないようになっている。

このようなストリームを、AVHDD1032がDVD装置1033に送信するさいの動作についてであるが、AVHDD1032の送信手段1035は、蓄積手段1034に蓄積されているストリームをDVD装置1033に送信するさい、ストリームを構成する各ブロックのデータパケットを、D4、D3、D2、D1、D0の順序で送信する。

DVD装置1033では、第5記録手段1036が、AVHDD1032からのデータをDVD1037に記録する。

DVD1037に記録されたデータを再生するときは、再生手段1038が、ストリームを構成する各ブロックについて、データパケットを、D0、D1、D2、D3、D4の順に再生していき、ストリーム全体を再生する。

このように、AVHDD1032からDVD装置1033に送信されるデータパケットが、D4、D3、D2、D1、D0の順に送信されるので、データ送信の途中で停電などで電源遮断されても、D4、D3、D2、D1、D0が送信されなければ、データパケットD0、D1、D2、D3、D4で構成されるブロックは再生されないで、送信データが他の装置に漏れた場合であっても、その送信データが他の装置において解読されるという状況を回避することができる。

なお、上述した実施の形態では、データパケットD0、D1、D2、D3

WO 01/48755

PCT/JP00/09260

108

、D 4の連鎖暗号化について詳述しなかったが、連鎖暗号化されたデータパケットD 0、D 1、D 2、D 3、D 4がAVHDD 1 0 3 2の蓄積手段1 0 3 4に蓄積されていてもよいし、AVHDD 1 0 3 2に連鎖暗号化を行う手段を設けて、AVHDD 1 0 3 2の送信手段1 0 3 5がストリームを送信しようとするさいに、各ブロックのデータパケットそれぞれについて連鎖暗号化させるようにしてもよい。

また、上述した実施の形態では、ストリームは、D 0、D 1、D 2、D 3、D 4の5個のデータパケットで構成されるブロック複数個で構成されたとしたが、各ブロックを構成するデータパケットの数は5個に限定されるものではない。また、ストリームは、複数個のブロックで構成されると限定されるものでもない。ストリームは、複数個のブロックで構成されておらず、複数個のデータパケットで構成されていてもよい。その場合、送信手段1 0 3 5は、ストリームを構成するデータパケットを、最後尾から先頭側に順に送信することになる。

また、上述した実施の形態では、ストリームの送信について説明したが、ストリームを移動させる場合には、データパケットD 0、D 1、D 2、D 3、D 4について着目すると、データパケットD 4、D 3、D 2、D 1の転送が完了したら、移動前の記録媒体からデータパケットD 1～D 4を消去し、その消去が完了した後にデータパケットD 0を転送し、移動前の記録媒体からデータパケットD 0を消去するとしてもよい。

なお、以上第8～第11の実施の形態では、CCIの値が、Copy Never、Copy once、No more CopyのいずれかであるAVデータを一括してコピー禁止データと呼んだが、以下第12～第16

WO 01/48755

PCT/JP00/09260

109

の実施の形態では、CCIがCopy neverであるAVデータなどの複製することが禁止されているコンテンツを複製禁止コンテンツと呼ぶことにする。

(第12の実施の形態)

図33は、本発明の第12の実施の形態による記録再生装置の構成図である。図に示すように、判別情報検出手段2010は、外部からの放送信号から、コピー制限に関する判別情報を検出するための手段、時間情報取得手段2011は、外部の放送信号から、時間に関する時間信号を取得するための手段、記録再生手段2012は、外部からの放送信号を記録再生するための手段、記録媒体2013は、ハードディスク等で実現される、記録再生が同時に可能であり、ランダム・アクセスが可能である、放送のデータを蓄積するための手段、制御入力インターフェイス（以下制御入力I/F）2015は、ユーザからの制御を受け付ける手段、切り替え手段2016は、記録再生手段2012からの入力と、外部からの放送の入力とを受け、いずれかを選択して外部のモニタ等へ出力する手段である。また、記録媒体2013において、記録バッファ2014は、コピー制限がなされたデータを専用に記録する領域である。なお、本実施の形態にて扱われる放送は、MPEGトランスポートストリームまたはMPEGプログラムストリーム（以下総称してMPEGストリームと呼ぶ）を用いたデジタル放送であり、デコード処理に関する手段等は省略するものとする。以下、各実施の形態も同様である。また、判別情報検出手段2010、時間情報取得手段2011、記録再生手段2012は本発明の記録手段の一例である。

以上のような構成を有する、本発明の第12の実施の形態による記録再生

WO 01/48755

PCT/JP00/09260

110

装置の動作について、以下に説明を行う。

はじめに、判別情報検出手段2010は、外部からMPEGストリームの入力を受けると、ヘッダまたはデータ列を構成する各パケットを参照して、コピーガードもしくはCCI (Copy Control Information) 等の著作権に関する情報を検出し、入力したコンテンツが、コピー禁止またはコピー制限が施されているものかどうかを判断する。今回の場合は、コピー禁止とされた複製禁止コンテンツのみが入力されているものとする。

次に、入力したMPEGストリームが、複製禁止コンテンツであることが判明すると、判別情報検出手段2010は、記録再生手段2012に対し、検出情報を出力する。検出情報の例としては、MPEGストリームに含まれる著作権情報や、コピーガード等がある。記録再生手段2012は、検出情報を受けると、これに基づき、記録媒体2013内の記録バッファ2014にMPEGストリームを記録するための準備を行う。

外部から、判別情報検出手段2010を介してMPEGストリームが入力すると、記録再生手段2012は、これを記録バッファ2014に記録する。

次に、記録再生手段2012による記録バッファ2014への記録動作の詳細について説明を行う。図34は、本第12の実施の形態による記録再生装置の動作を説明するためのタイムチャートである。図に示すように、本実施の形態の動作例として、記録バッファ2014に対し、放送時間90分に相当するデータ量を一時的に記録するための本実施の形態の記録再生装置を用い、生放送期間2020に放送されている放送時間120分の複製禁止コンテンツに対し、放送開始時刻から90分経過した後にタイムシフト再生に

WO 01/48755

PCT/JP00/09260

111

よる視聴を行うものとする。

はじめに、放送開始時刻になると、記録再生手段 2012 は記録バッファ 2014 に複製禁止コンテンツを構成するデータの記録を開始する。放送開始時刻以降、記録再生手段 2012 は、記録バッファ 2014 にデータを逐次記録し続けるが、再生は行わない。

一方、時間情報取得手段は、MPEG ストリームから、PCR パケットやタイムスタンプなどの時間情報を取得して、記録再生手段 2012 が複製禁止コンテンツを記録バッファ 2014 に記録開始した時点から、記録時間の計測を開始する。

次に、放送開始時刻から、時間情報取得手段 2011 の計測により記録期間 2021 (90 分) が経過すると、記録再生手段 2012 は、外部から入力される MPEG ストリームの逐次記録を継続しながら、放送開始時刻以降に記録したデータを記録バッファ 2014 上から消去開始する。ただし、今回の動作例においては、放送開始時刻から記録期間 2021 が経過した時刻は、タイムシフト再生による視聴期間 2024 が始まる視聴開始時刻となっているため、記録再生手段 2012 は、記録されたデータを消去する前に再生し、切り替え手段 2016 を介して外部モニタへ出力する。

すなわち、記録期間 2021 において記録されたデータのうち、最初の 30 分の部分 2022 a に相当するデータ (生放送期間 2020 a に放送されたコンテンツ) は、放送開始時刻から 90 分経過後、タイムシフト再生による視聴開始時刻とともに、再生 (タイムシフト再生による視聴期間 2024 a にて視聴されるコンテンツ) が行われ、その後直ちに消去されることになる。

WO 01/48755

PCT/JP00/09260

112

次に、タイムシフト再生による視聴開始時刻から記録再生期間 2022a が経過すると、記録再生手段 2012 は、記録再生期間 2022b として、データの逐次記録を放送終了時刻まで継続するとともに、既に記録バッファ 2014 内に蓄積したデータの再生を、データ部分 2022a から連続するようにして継続する。

次に、放送終了時刻になると、記録再生手段 2012 は、データの逐次記録を停止し、記録バッファ 2014 に記録されているデータの再生を、視聴終了時刻まで実行する（再生期間 2023）。

なお、以上の動作について、記録再生期間 2022b および再生期間 2023 においては、再生したデータは一旦記録バッファ 2014 上に保存しておいて、視聴終了時刻経過後、一括して消去するようにしてもよいが、事故により記録再生装置の電源が切れた場合など、データが記録媒体 2013 上に保存されてしまう事態を防ぐために、再生した直後に消去するのが望ましい。

また、視聴開始時刻を経過しても、タイムシフト再生が行われない場合は、記録再生手段 2012 は記録バッファ 2014 上に記録した全てのデータを消去する。これにより、複製禁止コンテンツをタイムシフト以外の形式で再生されることを防ぐことができる。

また、以上の説明においては、判別情報検出手段 2010 が複製禁止コンテンツのデータに含まれる判別情報を検出すると、記録再生手段 2012 が自動的にタイムシフト再生のための記録動作を開始するものとして説明を行ったが、記録再生手段 2012 の記録動作開始は、判別情報をきっかけとするものでなく、制御入力 I/F 2015 を介して、外部（ユーザ）からの制

WO 01/48755

PCT/JP00/09260

113

御によって行われるものとしてもよい。

また、以上の説明においては、記録期間 2021 の終了とタイムシフト再生による視聴開始時刻とを同時刻に設定し、複製禁止コンテンツのタイムシフト再生の動作と、該複製禁止コンテンツを構成するデータの消去の動作とを連動するものとして説明を行ったが、これに限定する必要はなく、図 35 に示すように、視聴開始時刻は、記録期間 2021 内（タイムシフト再生を任意の時刻に設定可能な期間 2024 c）でさえあれば、制御入力 I/F 2015 からの制御に基づき、任意の時刻に設定してよいし、時刻設定を行わず、記録再生手段 2012 への直接命令によって実行してもよい。このとき、記録期間 2021 内に、記録再生手段 2012 へのタイムシフト再生の直接命令が行われない場合は、記録再生手段 2012 は記録動作を停止するようにするのが好ましい（図 35 中の期間 2021 a）。また同時に、再びタイムシフト再生の直接命令が行われても、これを受付けないように設定するのが望ましい。

また、以上の動作において、記録期間 2021 を経過した場合、記録再生手段 2012 は、外部から入力される MPEG ストリームの逐次記録を継続しながら、放送開始時刻以降に記録したデータを記録バッファ 2014 上から消去するものとして説明を行ったが、再生不可能な状態に該データを書き換えた上で、記録バッファ 2014 上にデータを保持しておくようにしてもよい。

（第 13 の実施の形態）

本発明の第 13 の実施の形態による記録再生装置は、複製禁止コンテンツを記録するための記録バッファとして、リングバッファを用いたものである。

WO 01/48755

PCT/JP00/09260

114

図 3 6 は、本発明の本第 1 3 の実施の形態による記録再生装置の構成図である。図において、図 3 3 と同一部または相当部については、同一符号を附し説明を省略する。また、リングバッファ 2 0 4 4 は、同一領域に上書き記録を繰り返し行うことにより一定量のデータを一時記録する手段である。

以上のような構成を有する、本発明の第 1 3 の実施の形態による記録再生装置について、以下、その動作を説明する。

はじめに、判別情報検出手段 2 0 1 0 が、外部の M P E G プログラムストリームを参照して、複製禁止コンテンツを記録再生手段 2 0 1 2 がリングバッファ 2 0 4 4 に記録する動作については、第 1 2 の実施の形態と同様に行われる。

次に、記録再生手段 2 0 1 2 による、リングバッファ 2 0 4 4 への記録動作の詳細について説明を行う。先に説明したように、リングバッファ 2 0 4 4 は、記録媒体 2 0 1 3 上の特定領域であって、一定量のデータを記録すると、記録開始位置に戻って上書き記録を行うものである。このとき、リングバッファ 2 0 4 4 の大きさは、あらかじめ設定しておいてもよいし、判別情報検出手段 2 0 1 0 から取得した検出情報に基づいて設定されるようにしてもよいが、いずれの場合でも、リングバッファ 2 0 4 4 の大きさは、記録の対象となる複製禁止コンテンツを全て記録できないように設定される。例えば、複製禁止コンテンツの放送時間が 1 2 0 分であるとすれば、リングバッファ 2 0 4 4 は 9 0 分に相当する容量に設定されるようにする。

上記のように設定されたリングバッファ 2 0 4 4 に対し、記録再生手段 2 0 1 2 が複製禁止コンテンツの記録を開始する。

ここで図 3 7 は、本第 1 3 の実施の形態による記録再生装置の動作を説明

WO 01/48755

PCT/JP00/09260

115

するためのタイムチャートである。以下、図 3 7 を参照して、本第 1 3 の実施の形態の記録再生手段 2 0 1 2 とリングバッファ 2 0 4 4 との動作の詳細を説明する。ただし、図に示すように、本実施の形態の動作例の各時刻、各時間の設定は、図 3 4 に示す第 1 2 の実施の形態の場合と同様とする。

はじめに、放送開始時刻になると、記録再生手段 2 0 1 2 はリングバッファ 2 0 4 4 に複製禁止コンテンツを構成するデータの記録を開始する。放送開始時刻以降、記録再生手段 2 0 1 2 はリングバッファ 2 0 4 4 に設定した容量がいっぱいになるまでデータを逐次記録し続けるが、再生は行わない（記録期間 2 0 5 1）。

次に、放送開始時刻から記録期間 2 0 5 1 が経過し、リングバッファ 2 0 4 4 に設定した容量がいっぱいになると、記録再生手段 2 0 1 2 は、リングバッファ 2 0 4 4 上において、記録期間 2 0 5 1 の時点の記録位置から、記録開始位置に記録ヘッド（リングバッファポインタ）を戻し、新たなデータの上書き記録を行う。

また、今回の動作例においては、記録期間 2 0 5 1 の終了は、タイムシフト再生による視聴期間 2 0 5 4 の開始時刻と同一であるから、記録再生手段 2 0 1 2 は、外部から入力される M P E G ストリームの上書き記録を行うとともに、放送開始時刻から記録された、上書き直前のデータの再生を開始する。すなわち、記録期間 2 0 5 1 において記録されたデータのうち、最初の 3 0 分の部分 2 0 5 2 a に相当するデータ（生放送期間 2 0 5 0 a に放送されたコンテンツ）は、放送開始時刻から 9 0 分経過後、タイムシフト再生による視聴開始時刻とともに再生され、上書き記録により消去される。。

続いて、記録再生手段 2 0 1 2 は、データの逐次記録を放送終了時刻まで

WO 01/48755

PCT/JP00/09260

116

継続するとともに、データ再生を継続する（記録再生期間 2052b）。

次に、放送終了時刻になると、記録再生手段 2012 は、データの上書き記録を停止し、リングバッファ 2044 に記録されているデータの再生を、視聴終了時刻まで実行する（再生期間 2053）。

なお、以上の動作について、リングバッファ 2044 から再生したデータは、一旦リングバッファ 2044 上に保存しておいて、視聴終了時刻経過後、一括して消去するようにしてもよいが、事故により記録再生装置の電源が切れた場合など、データが記録媒体 2013 上に保存されてしまう事態を防ぐために、再生した直後に消去するのが望ましい。

また、視聴開始時刻を経過しても、タイムシフト再生が行われない場合は、記録再生手段 2012 はリングバッファ 2044 上に記録した全てのデータを消去する。これにより、複製禁止コンテンツをタイムシフト以外の形式で再生されることを防ぐことができる。

また、以上の動作においては、記録期間 2051 の終了とタイムシフト再生による視聴開始時刻とを同時刻に設定し、複製禁止コンテンツのタイムシフト再生の動作と、該複製禁止コンテンツを構成するデータの上書き記録の動作とを連動するものとして説明を行ったが、これに限定する必要はなく、図 38 に示すように、視聴開始時刻は、記録期間 2061 内（タイムシフト再生を任意の時刻に設定可能な期間 2064c）でさえあれば、制御入力 I/F 2015 からの制御に基づき、任意の時刻に設定してよいし、時刻設定を行わず、記録再生手段 2012 への直接命令によって実行してもよい。このとき、記録期間 2061 内に、記録再生手段 2012 へのタイムシフト再生の直接命令が行われない場合は、記録再生手段 2012 は記録動作を停止

WO 01/48755

PCT/JP00/09260

117

するようにするのが好ましい（図中の期間 2061a）。また同時に、再びタイムシフト再生の直接命令が行われても、これを受付けないように設定することが望ましい。

また、以上の動作においては、記録期間 2061 を経過した場合、記録再生手段 2012 は、外部から入力される MPEG ストリームの逐次記録を継続しながら、放送開始時刻以降に記録したデータを記録バッファ 2014 上から消去するものとして説明を行ったが、再生不可能な状態に該データを書き換えた上で、記録バッファ 2014 上にデータを保持しておくようにしてもよい。

また、本実施の形態によるタイムシフト再生において、データを再生する際のリングバッファ上の記録位置については、（１）リングバッファ 2044 上に上書き記録が行われていない状態での再生位置は、リングバッファ 2044 上にて記録が開始された位置と同一となり、（２）上書き記録が行われている状態での再生位置は、リングバッファ 2044 上にて、再生動作の制御が行われた時点の位置（上書き記録が最後に行われた位置）の直後となるようにする。すなわち、上記（１）（２）のいずれの場合においても、タイムシフト再生は、リングバッファ 2044 に記録されたもっとも古いデータから順に読み出しが行われるようにする。図 38 に示す例では、上記（１）は、期間 2064d（放送開始時刻以降 30 分）内にタイムシフト再生が行われた場合に相当し、再生開始位置は常に図中点 A に一意に決定される。上記（２）は、期間 2064e（放送開始時刻 30 分経過以降 60 分まで）内にタイムシフト再生が行われた場合に相当し、再生開始位置は、期間 2064e 上のリングバッファの記録ヘッド（バッファポインタ）の現在位置に

相当する。

(第 1 4 の実施の形態)

本発明の第 1 4 の実施の形態による記録再生装置は、複製禁止コンテンツと、複製可能なコンテンツとが混在する放送を受信する場合、複製禁止コンテンツだけを選択的にタイムシフト再生できるようにしたものである。

本実施の形態の構成は第 1 2 の実施の形態と同様であるので、説明には図 3 3 を用いる。また、図 3 9 は、本実施の形態による記録再生装置の動作を説明するための図である。ただし、本実施の形態においては、タイムシフト可能な時間を上記実施の形態の 9 0 分ではなく、1 2 0 分に設定したものとする。以下、図 3 9 を参照して、本発明の実施の形態の動作を説明する。

外部から入力される M P E G ストリーム 2 0 7 0 は、コピーが禁止された複製禁止コンテンツ 2 0 7 0 a および 2 0 7 0 c と、コピー可能な通常のコンテンツ 2 0 7 0 b および 2 0 7 0 d とが混在しており、時系列順に、複製禁止コンテンツ 2 0 7 0 a、コンテンツ 2 0 7 0 b、複製禁止コンテンツ 2 0 7 0 c、コンテンツ 2 0 7 0 d の順に記録再生装置に入力する。判別情報検出手段 2 0 1 0 は、各コンテンツに含まれる判別情報を取得して、記録再生手段 2 0 1 2 に出力し、時間情報取得手段は、各コンテンツ毎に時間情報を記録再生手段 2 0 1 2 へ出力する。判別情報および時間情報を取得した記録再生手段 2 0 1 2 は、これらに基づき、各コンテンツの放送時間が経過する毎に、複製禁止コンテンツは記録バッファ 2 0 1 4 に一時記録し、通常のコンテンツは記録媒体 2 0 1 3 内の、記録バッファ以外の記録領域に記録するようにする。

このとき、コンテンツの入力は時系列順となるので、図 3 9 に示すように

WO 01/48755

PCT/JP00/09260

119

、記録バッファ 2014 においては、はじめに複製禁止コンテンツ 2070 a、次いで複製禁止コンテンツ 2070 c が記録され、記録媒体 2013 においては、はじめにコンテンツ 2070 b、次いでコンテンツ 2070 d が記録される。

記録バッファ 2014 内に記録された複製禁止コンテンツ 2070 a および 2070 c は、第 12 の実施の形態と同様にして順々にタイムシフト再生される。タイムシフト再生終了後には記録バッファ 2014 からはデータが消去、または再生不可能な状態にされるが、記録媒体 2013 内に記録されたコンテンツ 2070 b および 2070 d は、恒久的に記録しておくことができる。

なお、上記の説明においては、本実施の形態は、第 12 の実施の形態の構成を有する記録再生装置において実現されるものとして説明を行ったが、第 13 の実施の形態の構成とした場合でも、同様に行うことができる。

(第 15 の実施の形態)

本発明の第 15 の実施の形態による記録再生装置は、一時的に記録された複製禁止コンテンツのデータを暗号化して、視聴することが不可能な状態にするものである。

図 40 は、本発明の第 15 の実施の形態の記録再生装置に用いられるデータ秘匿化手段 2080 の構成図である。図に示すように、記録バッファ 2014 は第 12 の実施の形態の記録バッファと同一手段、暗号化手段 2081 は記録再生手段 2012 から入力されるデータを時変キーにより暗号化する手段、復号化手段 2082 は記録バッファ 2014 から出力される暗号化されたデータを復号する手段、時変キー生成手段 2083 は暗号化手段 208

WO 01/48755

PCT/JP00/09260

120

1 および復号化手段 2082 にて用いる時変キーを生成する手段、キーバッファ 2084 は時変キーを一時蓄積する手段である。

以上のような構成を有する本実施の形態の動作を、以下に説明する。記録再生手段 2012 からデータが暗号化手段 2081 に入力されると、暗号化手段 2081 は、時変キー生成手段 2083 が生成した時変キーに基づき元データを暗号化する。暗号化されたデータは記録バッファ 2014 に記録される。

一方、時変キー生成手段 83 は、暗号化手段 2081 が取得したものと同一時変キーをキーバッファ 2084 に出力し、キーバッファ 2084 はこれを保持しておく。

次に、記録再生手段 2012 がタイムシフト再生を行い、記録バッファから暗号化したデータを復号化手段 2082 に出力すると、復号化手段はキーバッファ 2084 からデータの復号に必要なデータを取得して、該データの復号を行う。

上記の動作において、時変キーを一時的に格納するキーバッファは、記録バッファ 2014 のデータ容量の時間分と同一の時間分が越えると消滅するようにする。これにより、タイムシフト再生が行われなかったデータは、暗号化されたまま記録バッファ 2014 内に保持されることになり、再生することは可能でも、視聴することは不可能になる。

時変キーを消滅させるには、例えば、キーバッファ 2084 を、リングバッファ構成としておいて、キーバッファに蓄積されていくキーを常に新しいもので上書きするようにするとよい。リングバッファの容量としては、例えば、図 34 に示す第 12 の実施の形態の動作例であるならば、記録期間 20

21と同等とする。

また、タイマーを別途設けて時間を計測しておき、所定の時刻が経過するとキーバッファ2084から、設定した時刻以降のキーを逐次消去するようにしてもよい。

また、キーバッファ2084を揮発性メモリによって構成すると、記録再生装置の電源をオフにすると、キーバッファ内の全てのキーが消去され、これによっても秘匿性を確保することが可能となる。

(第16の実施の形態)

本発明の第16の実施の形態による記録再生装置は、タイムシフト再生のタイミングを、ユーザに告知できるようにしたものである。

図41は、本発明の本第16の実施の形態による記録再生装置の構成図である。図において、図33と同一部または相当部については、同一符号を附し説明を省略する。また、告知手段2091は、音声、画像または文字情報によって、該記録再生装置の動作状態を告知するための手段である。

また、図42は、本実施の形態による記録再生装置の動作を説明するための図である。以上のような構成を有する、本発明の第16の実施の形態による記録再生装置について、以下、その動作を説明する。ただし、記録バッファ2014に設定する容量は、第12の実施の形態と同様、放送時間90分に相当するものとし、その他、第12の実施の形態と重複する動作については説明を省略し、相違点のみを述べる。

はじめに、ユーザが放送局から放送される複製禁止コンテンツを生放送にて視聴しており、時刻tに何らかの理由で視聴を一時中断する場合を考える。このとき、ユーザは制御入力I/F2015から入力を行い、記録再生手段

WO 01/48755

PCT/JP00/09260

122

2012を起動させる。記録再生手段2012は、制御入力I/F2015からの入力を受けた時点（時刻t1と同一）から、記録バッファ2014に該複製禁止コンテンツの記録を開始する。一方、この間記録再生装置は「ポーズ」状態となる。

記録バッファ2014には、第12の実施の形態の動作と同様にして、複製禁止コンテンツのデータが記録されていくが、時刻t2になると、ユーザに対してアラーム音を発しユーザに対して記録再生装置に対して制御を行うよう注意を促す。本実施の形態においては、時刻t2は、記録時刻t1から、記録再生手段2012が記録バッファ2014に記録しているデータの、設定した容量に達するまでの残りの量（放送時間単位）と設定しており、本実施の形態では（放送時間単位で）5分とした。したがって時刻t2は、具体的には（記録開始（ポーズ開始）時刻+85分（記録バッファに一時記録された複製禁止コンテンツの量-5分））となる。

告知手段2091からの告知によって、ユーザは、制御入力I/F2015から入力を行い、ポーズを解除して、複製禁止コンテンツの視聴を再開する。ポーズ前と異なるのは、ユーザが視聴している複製禁止コンテンツは、放送局からの生放送ではなく、記録バッファ2014からタイムシフト再生されたものということである。

この場合、時刻t2から時刻t1までの間ポーズが行われることとなり、ユーザの番組視聴終了時刻t6は、実際の放送の終了時刻t4よりこの（t2-t1）分だけ遅れたものになる。

また、この動作において時刻t2からタイムシフト再生が行われると、放送局から番組が放送されている間に、記録バッファ2014に一時記録され

WO 01/48755

PCT/JP00/09260

123

ていたコンテンツは再生が終了するが、この再生終了時刻 t_7 から番組視聴終了時刻 t_6 までは、記録バッファ 2014 には、データの記録再生が行われるとともに、再生した番組データが視聴不可能な状態として保持されているか、消去されていることとなっている。

一方、時刻 t_2 を経過しても制御入力 I/F 2015 にユーザからの入力が行われない場合は、記録バッファ 2014 に、設定された時間分のデータが全て記録される時刻 t_3 で、記録バッファ 2014 への一時記録動作は停止するとともに、強制的にタイムシフト再生が開始される。本実施の形態では、告知手段 2091 が告知を行った時刻 t_2 から 5 分経過した時刻 t_3 がこの時刻に相当する。この動作において、時刻 t_3 から、ポーズが開始された時刻 t_1 の差だけ遅れて、番組はタイムシフト再生されていることとなり、ユーザの番組視聴が終了する時刻 t_5 は、実際の放送の終了時刻 t_4 よりこの $(t_3 - t_1)$ 分だけ遅れたものになる。また、この $(t_3 - t_1)$ 分は、はじめに記録バッファ 2014 に設定された複製禁止コンテンツの記録時間と同一である。さらに、時刻 t_3 以降の放送は記録バッファ 2014 には記録されていない。したがって、強制的なタイムシフト再生の終了時刻 t_8 から、番組視聴終了時刻 t_5 までの間は、既に番組が放送終了した後に放送される別の番組をユーザは視聴することになるか、タイムシフト再生の終了時刻 t_8 がそのままユーザの視聴時刻となる。

つまり、時刻 t_2 を経過してもユーザからタイムシフト再生の入力が行なわれずに、一旦強制的にタイムシフト再生が開始されると、ユーザはポーズ前から視聴されていた番組を、ポーズ解除後は完全な形で視聴することができないことになる。

WO 01/48755

PCT/JP00/09260

124

以上のように、本実施の形態によれば、ユーザが所望の時間に複製禁止コンテンツのタイムシフト再生を設定できるとともに、複製禁止コンテンツの著作権を保護するために、所定の時間が経過するまでに、ユーザにタイムシフト再生の完全な実行を促すことができる。

なお、上記の実施の形態においては、記録バッファ 2014 を用いた例にて説明を行ったが、記録バッファ 2014 の代わりに第 13 の実施の形態のリングバッファ 2044 を用いても同様の効果が得られる。リングバッファ 2044 を用いた場合の動作は、図 42 の一点鎖線部に示すように、時刻 t_4 から t_3 までの間、リングバッファである記録バッファには、データの上書き記録を続けながら同時に再生が行われることにより、バッファの設定時間分のタイムシフト再生が行われることとなる。ただし、時刻 t_3 で上書き動作を禁じるように設定した場合の動作は、上述した通常の記録バッファの強制的なタイムシフト再生実行の場合と同様となる。

また、本実施の形態の構成は、既に述べた第 14 の実施の形態と組み合わせ用いてもよい。

さらに、上記の各実施の形態においては、本発明の記録装置と再生手段とを一体化した記録再生手段が記録バッファへの記録および再生を行うものとして説明を行ったが、本発明の構成はこれに限定するものではなく、記録を行う記録手段のみを備えたものとして、記録バッファ 2014 またはリングバッファ 2044 からデータ再生を行う手段は、外部装置として別途設けるようにしてもよい。

さらに、上記の各実施の形態において、複製禁止コンテンツの記録期間等は、時間情報として、コンテンツの MPEG ストリーム内の PCR パケット

をカウントする計測を行ったが、時間情報はこれに限定するものではなく、他の時間情報としてはE P Gを用いてもよく、取得したE P Gを参照して、別途設けたタイマによって絶対時刻測定を行うことにより、計測を行ってもよい。

さらに、この時間情報は、記録媒体2013にて計測されているものであってもよい。

さらに、この時間情報は、本発明の実施の形態の記録再生装置にM P E Gストリームを入力するS T B等の機器内にて計測されているものであつて、M P E Gストリームとともに入力するようにしてもよい。さらにこれら時間情報は、一時記録の対象となるコンテンツの放送開始時刻等を含むものであつても良い。

さらに、上記の各実施の形態において、複製禁止コンテンツは、一度の複製も許されないデータからなるものとして説明を行ったが、本発明の複製制限コンテンツはこれに限定するものではなく、一度だけ複製が許可されたデータからなるコンテンツを対象としてもよい。要するに、本発明は、複製が禁止または所定の制限が附されたデータに対してなら何でも用いることが可能である。

なお、本明細書には、上述した本発明の記録装置によってディスク記録された暗号化されたデータを再生するよう制御する制御手段と、前記制御手段によって制御され、前記データを再生する再生手段と、前記再生されたデータを復号してインターフェースに送る復号手段とを備え、前記制御手段は、前記コピー許諾情報を前記記録手段が再生するように前記記録手段を制御し、前記復号手段は、前記デバイスユニークキーと前記コピー許諾情報の少なくともいずれかを含む第1

の情報を作成し、前記復号手段は、前記記録ユニット情報を用いて、前記第1の情報を復号した情報であるコンテンツキーを生成し、前記復号手段は、前記コンテンツキーを用いて前記データを復号することを特徴とする再生装置に関する発明も記載されている。

さらに、本明細書には、上述した本発明の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、前記制御手段によって制御され、前記データを再生する再生手段と、前記再生されたデータを復号してインターフェースに送る復号手段とを備え、前記制御手段は、前記暗号化されたタイトルキーを前記記録手段が再生するように前記記録手段を制御し、前記復号手段は、前記暗号化されたタイトルキーを前記デバイスユニークキーを用いて復号することを特徴とする再生装置に関する発明も記載されている。

さらに、本明細書には、上述した本発明の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、前記制御手段によって制御され、前記データを再生する再生手段と、前記再生されたデータを復号してインターフェースに送る復号手段とを備え、前記復号手段は、前記タイトルキーを用いて前記データを復号することを特徴とする再生装置に関する発明も記載されている。

さらに、本明細書には、上述した本発明の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、前記制御手段によって制御され、前記データを再生する再生手段と、前記再生されたデータを復号してインターフェースに送る復号手段とを備え、前記制御手段は、前記暗号化されたタイトルキーを前記記録手段が再生するように前記記録手段を制御し、前記復号手段は、前記再生されたタイトルキーを前記デバイスユニークキーを用いて

WO 01/48755

PCT/JP00/09260

127

復号し、前記復号手段は、前記タイトルキーを含む第3の情報を作成し、前記制御手段が前記記録手段に連続してアクセスする最小単位である記録ユニットを前提とする記録ブロックに固有の番号及び／または記号である記録ユニット情報を用いて、前記復号手段は、前記第3の情報を復号した情報であるコンテンツキーを生成し、前記復号手段は、前記コンテンツキーを用いて前記データを復号することを特徴とする再生装置に関する発明も記載されている。

さらに、本明細書には、上述した本発明の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、前記制御手段によって制御され、前記データを再生する再生手段と、前記再生されたデータを復号してインターフェースに送る復号手段とを備え、前記復号手段は、前記コピー許諾情報を用いて前記データを復号することを特徴とする再生装置に関する発明も記載されている。

さらに、本明細書には、上述した本発明の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、前記制御手段によって制御され、前記データを再生する再生手段と、前記再生されたデータを復号してインターフェースに送る復号手段とを備え、前記制御手段は、前記暗号化されたタイトルキーを前記記録手段が再生するように前記記録手段を制御し、前記復号手段は、前記再生されたタイトルキーを前記デバイスユニークキーを用いて復号し、前記制御手段は、前記コピー許諾情報を前記記録手段が再生するように前記記録手段を制御し、前記復号手段は、前記タイトルキーと前記コピー許諾情報の少なくともいずれかをを含む第2の情報を作成し、前記制御手段が前記記録手段に連続してアクセスする最小単位である記録ユニットに対応する記録ブロックに固有の番号及び／または記号である記録ユニット情報を用いて、前記復号手

段は、前記第2の情報を復号した情報であるコンテンツキーを生成し、前記復号手段は、前記コンテンツキーを用いて前記データを復号することを特徴とする再生装置に関する発明も記載されている。

さらに、本明細書には、上述した本発明の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、前記制御手段によって制御され、前記データを再生する再生手段と、前記再生されたデータを復号してインターフェースに送る復号手段とを備え、前記制御手段は、前記コピー許諾情報を再生するよう前記記録手段を制御し、前記復号手段は、前記データを前記再生されたコピー許諾情報を用いて復号することを特徴とする再生装置に関する発明も記載されている。

さらに、本明細書には、上述した本発明の全部または一部の手段の全部または一部の機能をコンピュータにより実行させるためのプログラム及び／またはデータを担持した媒体であり、コンピュータにより読み取り可能且つ、読み取られた前記プログラム及び／またはデータが前記コンピュータと協働して前記機能を実行する媒体に関する発明も記載されている。

さらに、本明細書には、上述した本発明の全部または一部の手段の全部または一部の機能をコンピュータにより実行させるためのプログラム及び／またはデータである情報集合体であり、コンピュータにより読み取り可能且つ、読み取られた前記プログラム及び／またはデータが前記コンピュータと協働して前記機能を実行する情報集合体に関する発明も記載されている。

さらに、データとは、データ構造、データフォーマット、データの種類のどれを含む。

さらに、媒体とは、ROM等の記録媒体、インターネット等の伝送媒体、

WO 01/48755

PCT/JP00/09260

129

光・電波・音波等の伝送媒体を含む。

さらに、担持した媒体とは、例えば、プログラム及び／またはデータを記録した記録媒体、やプログラム及び／またはデータを伝送する伝送媒体等を含む。

さらに、コンピュータにより処理可能とは、例えば、ROMなどの記録媒体の場合であれば、コンピュータにより読みとり可能であることであり、伝送媒体の場合であれば、伝送対象となるプログラム及び／またはデータが伝送の結果として、コンピュータにより取り扱えることであることを含む。

さらに、情報集合体とは、例えば、プログラム及び／またはデータ等のソフトウェアを含むものである。

さらに、以上説明した様に、本発明の構成は、ソフトウェア的に実現しても良いし、ハードウェア的に実現しても良い。

産業上の利用可能性

以上説明したところから明らかなように、本発明は、著作権保護が必要なデータを記録する場合及び／または著作権保護が必要なデータを再生する場合に著作権を保護することが出来る記録装置及び再生装置とを提供することが出来る。

また、本発明は、著作権を保護しつつ、コピーが禁止されているデータを他の記録媒体に移動させるまたは複写するデータ処理装置と、そのデータ処理装置からのデータを記録媒体に記録し、または記録するとともに再生する記録再生装置と、著作権を保護してデータをバックアップしておく暗号化データ復号記録装置システムおよびそのシステムを構成する復号記録装置、記

WO 01/48755

PCT/JP00/09260

130

録装置と、著作権を保護してデータを送信するデータ送信装置とを提供することができる。

また、本発明は、複製が禁じられた放送番組等を、著作権侵害を回避するようにしてタイムシフト再生を行うことが出来る記録装置及び記録再生装置とを提供することが出来る。

WO 01/48755

PCT/JP00/09260

131

請 求 の 範 囲

1. インターフェースから送られてくるデータを暗号化する暗号化手段と、
前記暗号化されたデータを記録するよう制御する制御手段と、
前記制御手段によって制御され、前記暗号化されたデータをディスクに記録する記録手段とを備えたことを特徴とする記録装置。
2. 前記暗号化手段は、記録装置自らに割り付けられた固有の数値及び／または記号であるデバイスユニークキーを用いて、前記データを暗号化することを特徴とする請求項 1 記載の記録装置。
3. 前記暗号化手段は、前記制御手段が前記記録手段に連続してアクセスする最小単位である記録ユニットに対応する記録ブロックに固有の番号及び／または記号である記録ユニット情報を用いて、前記データを暗号化することを特徴とする請求項 1 または 2 に記載の記録装置。
4. 前記記録ユニット情報を用いて、前記データを暗号化するとは、前記記録ユニット情報に基づいて得られたキーで前記データを暗号化することであることを特徴とする請求項 3 記載の記録装置。
5. 少なくとも前記記録ブロックに記録される前記暗号化されたデータ及び前記暗号化されたデータに付加された付加情報は、すべての部分が暗号化されて前記記録手段に記録されることを特徴とする請求項 3 または 4 に記載の記録装置。
6. 前記データには、コピー許諾情報が付加されており、
前記制御手段は、前記コピー許諾情報を前記記録手段が記録するように前記記録手段を制御し、
前記暗号化手段は、前記デバイスユニークキーと前記コピー許諾情報の少なく

WO 01/48755

PCT/JP00/09260

132

ともいづれかを含む第 1 の情報を作成し、

前記記録ユニット情報を用いて、前記暗号化手段は、前記第 1 の情報を暗号化した情報であるコンテンツキーを生成し、

前記暗号化手段は、前記コンテンツキーを用いて前記データを暗号化し、

前記制御手段は前記暗号化したデータを前記記録手段が記録するように前記記録手段を制御することを特徴とする請求項 3～5 のいずれかに記載の記録装置。

7. 前記データには、前記データに固有の数値及び／または記号であるタイトルキーが割り付けられており、

前記暗号化手段は、前記タイトルキーを前記デバイスユニークキーを用いて暗号化し、

前記制御手段は、前記暗号化されたタイトルキーを前記記録手段に記録するように前記記録手段を制御することを特徴とする請求項 2 記載の記録装置。

8. 前記暗号化手段は、前記タイトルキーを用いて前記データを暗号化することを特徴とする請求項 7 記載の記録装置。

9. 前記暗号化手段は、前記タイトルキーを前記デバイスユニークキーを用いて暗号化し、

前記制御手段は、前記暗号化されたタイトルキーを前記記録手段が記録するように前記記録手段を制御し、

前記暗号化手段は、前記タイトルキーを含む第 3 の情報を作成し、

前記制御手段が前記記録手段に連続してアクセスする最小単位である記録ユニットを前提とする記録ブロックに固有の番号及び／または記号である記録ユニット情報を用いて、前記暗号化手段は、前記第 3 の情報を暗号化した情報であるコンテンツキーを生成し、

前記暗号化手段は、前記コンテンツキーを用いて前記データを暗号化し、
前記制御手段は前記暗号化したデータを前記記録手段が記録するように前記記録手段を制御することを特徴とする請求項 8 記載の記録装置。

10. 前記データには、コピー許諾情報が付加されており、
前記暗号化手段は、前記コピー許諾情報をも用いて、前記データを暗号化することを特徴とする請求項 8 記載の記録装置。

11. 前記暗号化手段は、前記タイトルキーを前記デバイスユニークキーを用いて暗号化し、
前記制御手段は、前記暗号化されたタイトルキーを前記記録手段が記録するように前記記録手段を制御し、
前記制御手段は、前記コピー許諾情報を前記記録手段が記録するように前記記録手段を制御し、

前記暗号化手段は、前記タイトルキーと前記コピー許諾情報の少なくともいずれかを含む第 2 の情報を作成し、

前記制御手段が前記記録手段に連続してアクセスする最小単位である記録ユニットを前提とする記録ブロックに固有の番号及び／または記号である記録ユニット情報を用いて、前記暗号化手段は、前記第 2 の情報を暗号化した情報であるコンテンツキーを生成し、

前記暗号化手段は、前記コンテンツキーを用いて前記データを暗号化し、
前記制御手段は前記暗号化したデータを前記記録手段が記録するように前記記録手段を制御することを特徴とする請求項 10 記載の記録装置。

12. 前記暗号化手段は、コピー許諾情報が付加され、インターフェースから送られてくるデータを前記コピー許諾情報を用いて暗号化し、

WO 01/48755

PCT/JP00/09260

134

前記制御手段は、前記記録手段が前記データを記録する前及び／または前記データを記録した後に、前記コピー許諾情報を記録するよう前記記録手段を制御することを特徴とする請求項 1 記載の記録装置。

13. 前記制御手段は、少なくとも前記記録手段が前記データを記録する前に、前記コピー許諾情報を記録するよう前記記録手段を制御することを特徴とする請求項 1 2 記載の記録装置。

14. 前記制御手段は、前記記録手段が前記データを記録した後のみに、前記コピー許諾情報を記録するよう前記記録手段を制御することを特徴とする請求項 1 2 記載の記録装置。

15. インターフェースから送られてくる暗号化されたデータを記録するよう制御する制御手段と、

前記制御手段によって制御され、前記暗号化されたデータをディスクに記録する記録手段とを備えたことを特徴とする記録装置。

16. 請求項 1 記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

前記再生されたデータを復号してインターフェースに送る復号手段とを備えたことを特徴とする再生装置。

17. 請求項 2 記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

前記再生されたデータを復号してインターフェースに送る復号手段とを備え、

前記復号手段は、前記デバイスユニークキーを用いて前記再生されたデータを

WO 01/48755

PCT/JP00/09260

135

復号することを特徴とする再生装置。

18. 請求項3記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

前記再生されたデータを復号してインターフェースに送る復号手段とを備え、

前記復号手段は、前記記録ユニット情報を用いて前記再生されたデータを復号することを特徴とする再生装置。

19. 請求項4記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

前記再生されたデータを復号してインターフェースに送る復号手段とを備え、

前記復号手段は、前記記録ユニット情報に基づいて得られたキーで前記再生されたデータを復号することを特徴とする再生装置。

20. 請求項14記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段と、

前記再生されたデータを復号してインターフェースに送る復号手段とを備え、

前記データの記録時に、前記コピー許諾情報が前記記録手段に正常に記録出来なかった場合、前記復号手段は、前記コピー許諾情報が各値を取ると仮定して前記暗号化されたデータの全部または一部の復号を試行し、

前記試行した結果、前記再生されたデータが正常に復号出来た場合の前記コピー許諾情報の値を用いて前記再生されたデータを復号することを特徴とする再生装置。

WO 01/48755

PCT/JP00/09260

136

21. 請求項15記載の記録装置によってディスクに記録された暗号化されたデータを再生するよう制御する制御手段と、

前記制御手段によって制御され、前記データを再生する再生手段とを備え、

前記再生されたデータは、インターフェースに送られることを特徴とする再生装置。

22. 前記インターフェース、前記暗号化手段及び前記制御手段が、同一プリント基板上に一体化して配設されていることを特徴とする請求項1～14のいずれかに記載の記録装置。

23. 前記インターフェース、前記暗号化手段及び前記制御手段は、1チップ化されていることを特徴とする請求項22記載の記録装置。

24. 前記インターフェース、前記復号手段及び前記制御手段が同一プリント基板上に一体化して配設されていることを特徴とする請求項16～20のいずれかに記載の再生装置。

25. 前記インターフェース、前記復号手段及び前記制御手段は、1チップ化されていることを特徴とする請求項24記載の再生装置。

26. 第3者がデータとして再生出来る信号を出力している、前記プリント基板上の端子から検出される信号は、全て暗号化されているか及び／または非公開のフォーマットで記述されていることを特徴とする請求項22記載の記録装置。

27. 第3者がデータとして再生出来る信号を出力している、前記プリント基板上の端子から検出される信号は、全て暗号化されているか及び／または非公開のフォーマットで記述されていることを特徴とする請求項24記載の再生装置。

28. 第3者がデータとして再生出来る信号を出力している、前記プリント基板上の端子の性質は、非公開のフォーマットで定められていることを特徴とす

WO 01/48755

PCT/JP00/09260

137

る請求項 22 記載の記録装置。

29. 第3者がデータとして再生出来る信号を出力している、前記プリント基板上の端子の性質は、非公開のフォーマットで定められていることを特徴とする請求項 24 記載の再生装置。

30. 前記デバイスユニークキーは、外部の機器がアクセスすることが出来ないことを特徴とする請求項 2～11 のいずれかに記載の記録装置。

31. 前記コピー許諾情報は、前記記録手段のユーザから直接アクセスできないシステム領域に記録されることを特徴とする請求項 6、10、11、12、13、14 のいずれかに記載の記録装置。

32. 前記インターフェースから送られてくるデータには、コピー許諾情報が付加されており、

前記制御手段は、所定の条件のもとで、前記データの前記コピー許諾情報が、複製禁止 (copy never) を表す場合であっても、前記記録手段が前記データを記録するように制御することが出来ることを特徴とする請求項 1～15、22、23、26、28、30、31 のいずれかに記載の記録装置。

33. 前記所定の条件とは、記録された前記データが所定の時間後に再生不可となる場合であることを特徴とする請求項 32 記載の記録装置。

34. 前記所定の条件とは、記録された前記データが課金条件によって再生不可となる場合であることを特徴とする請求項 32 記載の記録装置。

35. 前記記録された暗号化されたデータには、コピー許諾情報が付加されており、

前記制御手段は、所定の条件のもとで、前記データの前記コピー許諾情報が、複製禁止 (copy never) を表す場合、前記再生手段が前記データを少

WO 01/48755

PCT/JP00/09260

138

なくとも1回再生するよう制御することを特徴とする請求項16～21、24、25、27、29のいずれかに記載の再生装置。

36. 前記所定の条件とは、記録された前記データが所定の時間後に再生不可となる場合であることを特徴とする請求項35記載の再生装置。

37. 前記所定の条件とは、記録された前記データが課金条件によって再生不可となる場合であることを特徴とする請求項35記載の再生装置。

38. 前記記録された暗号化されたデータには、コピー許諾情報が付加されており、

前記制御手段は、所定の条件のもとで、前記データの前記コピー許諾情報が、1回だけ複製することを許可(copy once)することを表す場合、前記記録手段により1回複製された後の前記データの前記コピー許諾情報が、再び1回だけ複製することを許可(copy once)することを表すようにして、前記再生手段が前記データを1回だけ複製出力するよう制御することを特徴とする請求項16～21、24、25、27、29のいずれかに記載の再生装置。

39. 前記所定の条件とは、前記再生手段が前記データを複製出力した所定の時間後に、前記データもしくは前記データの暗号化に用いたキーを消去する場合であることを特徴とする請求項38記載の再生装置。

40. 前記所定の条件とは、1回だけ複製出力された前記データの記録先がバックアップ用として前記データを記録する装置である場合であることを特徴とする請求項38記載の再生装置。

41. 前記記録先でバックアップ用として記録された前記データは、前記記録先では再生不可であることを特徴とする請求項40記載の再生装置。

42. 前記記録先でバックアップ用として記録された前記データは、元の再

WO 01/48755

PCT/JP00/09260

139

生装置に戻さない限り再生不可であることを特徴とする請求項 40 記載の再生装置。

43. 前記暗号化手段は、前記インターフェースから送られてくるデータのコピー許諾情報の値に関係なく前記データを暗号化することを特徴とする請求項 1～14、22、23、26、30～34 のいずれかに記載の記録装置。

44. 前記暗号化手段は、前記インターフェースから送られてくるデータのコピー許諾情報が自由に複製してもよいこと (Copy free) を表す場合、前記データを暗号化せず、

前記制御手段は、前記記録手段が前記暗号化されていないデータを記録するように制御することを特徴とする請求項 1～14、22、23、26、30～34 のいずれかに記載の記録装置。

45. データが記録される記録媒体に記録されているデータを他の記録装置へ移動させる移動手段を少なくとも備えたデータ処理装置であって、

前記移動手段が移動させようとするデータがコピーが禁止されているコピー禁止データである場合、そのコピー禁止データは、少なくとも前記データ処理装置から出力するときには、前記データ処理装置固有の暗号化鍵で暗号化されている

ことを特徴とするデータ処理装置。

46. データが記録される記録媒体に記録されているデータを他の記録装置に複写する複写手段を少なくとも備えたデータ処理装置であって、

前記複写手段が複写しようとするデータがコピーが禁止されているコピー禁止データである場合、そのコピー禁止データは、少なくとも前記データ処理装置から出力するときには、前記データ処理装置固有の暗号化鍵で暗号化

されている

ことを特徴とするデータ処理装置。

47. 前記コピー禁止データを前記暗号化鍵で暗号化する暗号化手段をさらに備えたことを特徴とする請求項45または46に記載のデータ処理装置。

48. 前記暗号化鍵で暗号化されている前記コピー禁止データを、前記暗号化鍵を用いて解読し、前記コピー禁止データを再生する再生手段をさらに備えたことを特徴とする請求項45～47のいずれかに記載のデータ処理装置。

49. 前記再生手段は、ユーザが視聴するさいに必要な速度で前記コピー禁止データを再生する手段であって、

前記他の記録装置から前記ユーザが視聴するさいに必要な速度よりも速い速度で、前記暗号化鍵で暗号化されている前記コピー禁止データが送信されてきた場合、送信されてきた前記コピー禁止データを、前記ユーザが視聴するさいに必要な速度よりも速い速度で格納する格納手段をさらに備え、

前記再生手段は、前記格納手段が前記他の記録装置からの前記コピー禁止データを格納するさいに、前記格納手段に格納された前記コピー禁止データもしくは、予め前記格納手段に格納されたデータを再生することができる

ことを特徴とする請求項48に記載のデータ処理装置。

50. 前記他の記録装置が、第2の記録媒体へデータを記録することができる装置であって、

前記第2の記録媒体が前記データ処理装置に対応する記録媒体であるか否かを判断する判断手段をさらに備え、

WO 01/48755

PCT/JP00/09260

141

前記移動手段または前記複写手段は、前記判断手段によって、前記第 2 の記録媒体が前記データ処理装置に対応する記録媒体であると判断された場合、前記コピー禁止データを移動させるまたは複写する

ことを特徴とする請求項 45～49 のいずれかに記載のデータ処理装置。

51. 前記他の記録装置が、第 2 の記録媒体へデータを記録することができる装置であって、

前記他の記録装置が前記データ処理装置に対応する装置であるか否かを判断する判断手段をさらに備え、

前記移動手段または前記複写手段は、前記判断手段によって、前記他の記録装置が前記データ処理装置に対応する装置であると判断された場合、前記コピー禁止データを移動させるまたは複写する

ことを特徴とする請求項 45～49 のいずれかに記載のデータ処理装置。

52. 前記移動手段または前記複写手段は、前記コピー禁止データを移動させるまたは複写するさい、そのコピー禁止データを 1 回だけコピー可能なデータとして出力することを特徴とする請求項 45～51 のいずれかに記載のデータ処理装置。

53. 請求項 45～47 のいずれかに記載のデータ処理装置からの前記暗号化鍵で暗号化されている前記コピー禁止データを、第 2 の記録媒体に記録する記録手段を備えたことを特徴とする記録再生装置。

54. 請求項 48 記載のデータ処理装置からの前記暗号化鍵で暗号化されている前記コピー禁止データを、第 2 の記録媒体に記録する記録手段と、

前記第 2 の記録媒体に記録された、前記暗号化鍵で暗号化されている前記コピー禁止データを、前記暗号化鍵で暗号化されているまま前記データ処理

WO 01/48755

PCT/JP00/09260

142

装置に送信する送信手段とを備えた

ことを特徴とする記録再生装置。

55. 請求項50または51に記載のデータ処理装置からの前記暗号化鍵で暗号化されている前記コピー禁止データを、前記第2の記録媒体に記録する記録手段と、

前記第2の記録媒体に記録された、前記暗号化鍵で暗号化されている前記コピー禁止データを、前記暗号化鍵で暗号化されているまま前記データ処理装置に送信する送信手段とを備えた

ことを特徴とする記録再生装置。

56. 請求項45、46、47、50、51のいずれかに記載のデータ処理装置からの前記暗号化鍵で暗号化されている前記コピー禁止データを、第2の記録媒体に記録する記録手段と、

前記第2の記録媒体に記録された、前記暗号化鍵で暗号化されている前記コピー禁止データを、前記暗号化鍵を用いて解読し、前記コピー禁止データを再生する解読再生手段とを備えた

ことを特徴とする記録再生装置。

57. 前記暗号化鍵が記録されている暗号化鍵記録媒体を再生する鍵再生手段と、

前記鍵再生手段が再生した前記暗号化鍵を記憶する鍵記憶手段とをさらに備え、

前記解読再生手段は、前記鍵記憶手段が記憶している前記暗号化鍵を利用して、前記コピー禁止データを再生する

ことを特徴とする請求項56記載の記録再生装置。

WO 01/48755

PCT/JP00/09260

143

58. 前記データ処理装置から送信されてきた前記暗号化鍵を受信する受信手段をさらに備え、

前記解読再生手段は、前記受信手段によって受信された前記暗号化鍵を利用して、前記コピー禁止データを再生する

ことを特徴とする請求項56記載の記録再生装置。

59. データが記録される記録媒体に記録されているデータを、他の記録装置へ、その他の記録装置において解読される形式のデータとして移動させる移動手段を少なくとも備え、

前記移動手段が移動させようとするデータがコピーが禁止されているコピー禁止データである

ことを特徴とするデータ処理装置。

60. データが記録される記録媒体に記録されているデータを、他の記録装置に、その他の記録装置において解読される形式のデータとして複写する複写手段を少なくとも備え、

前記複写手段が複写しようとするデータがコピーが禁止されているコピー禁止データである

ことを特徴とするデータ処理装置。

61. 前記他の記録装置において解読される形式のデータとは、平文データ、または前記他の記録装置固有の鍵で暗号化されたデータ、または前記他の記録装置における第2の記録媒体に付されている鍵で暗号化されたデータを意味することを特徴とする請求項59または60に記載のデータ処理装置。

62. 前記他の記録装置において解読される形式のデータが、さらに、

WO 01/48755

PCT/JP00/09260

144

前記他の記録装置において用いられるフォーマットのデータでもあることを特徴とする請求項 6 1 記載のデータ処理装置。

6 3. 前記他の記録装置が、第 2 の記録媒体へデータを記録することができる装置であって、

前記第 2 の記録媒体が前記データ処理装置に対応する記録媒体であるか否かを判断する判断手段をさらに備え、

前記移動手段または前記複写手段は、前記判断手段によって、前記第 2 の記録媒体が前記データ処理装置に対応する記録媒体であると判断された場合、前記コピー禁止データを移動させるまたは複写する

ことを特徴とする請求項 5 9 ～ 6 2 のいずれかに記載のデータ処理装置。

6 4. 前記第 2 の記録媒体に、前記第 2 の記録媒体が前記データ処理装置に対応する記録媒体であることを示す鍵が付されている場合、前記判断手段は前記鍵を用いて前記判断を行い、

前記判断手段によって、前記第 2 の記録媒体が前記データ処理装置に対応する記録媒体であると判断された場合、前記コピー禁止データを前記鍵を用いて暗号化する暗号化手段をさらに備え、

前記移動手段または前記複写手段は、前記暗号化された前記コピー禁止データを移動させるまたは複写する

ことを特徴とする請求項 6 3 記載のデータ処理装置。

6 5. 前記他の記録装置が、第 2 の記録媒体へデータを記録することができる装置であって、

前記他の記録装置が前記データ処理装置に対応する装置であるか否かを判断する判断手段をさらに備え、

WO 01/48755

PCT/JP00/09260

145

前記移動手段または前記複写手段は、前記判断手段によって、前記他の記録装置が前記データ処理装置に対応する装置であると判断された場合、前記コピー禁止データを移動させるまたは複写する

ことを特徴とする請求項 59～62 のいずれかに記載のデータ処理装置。

66. 前記他の記録装置が、前記データ処理装置に対応する装置であることを示す鍵を有している場合、前記判断手段は前記鍵を用いて前記判断を行い、

前記判断手段によって、前記他の記録装置が前記データ処理装置に対応する装置であると判断された場合、前記コピー禁止データを前記鍵を用いて暗号化する暗号化手段をさらに備え、

前記移動手段または前記複写手段は、前記暗号化された前記コピー禁止データを移動させるまたは複写する

ことを特徴とする請求項 65 記載のデータ処理装置。

67. 前記移動手段または前記複写手段は、前記コピー禁止データを移動させるまたは複写するさい、そのコピー禁止データを 1 回だけコピー可能なデータとして出力することを特徴とする請求項 59～66 のいずれかに記載のデータ処理装置。

68. 請求項 59 または 60 に記載のデータ処理装置からの前記コピー禁止データを第 2 の記録媒体に記録し、再生する記録再生装置であって、

前記コピー禁止データが平文データであり、

前記コピー禁止データを、前記第 2 の記録媒体に付されている暗号化鍵を用いて、または前記記録再生装置固有の暗号化鍵を用いて暗号化する暗号化手段と、

WO 01/48755

PCT/JP00/09260

146

前記暗号化手段によって暗号化された前記コピー禁止データを前記第 2 の記録媒体に記録する記録手段と、

前記第 2 の記録媒体に記録された、前記暗号化された前記コピー禁止データを、前記鍵を利用して解読し、再生する再生手段とを備えたことを特徴とする記録再生装置。

69. 請求項 59 または 60 に記載のデータ処理装置からの前記コピー禁止データを第 2 の記録媒体に記録し、再生する記録再生装置であって、

前記コピー禁止データが前記記録再生装置固有の鍵で暗号化されたデータ、または前記第 2 の記録媒体に付されている鍵で暗号化されたデータであり、

前記暗号化された前記コピー禁止データを前記第 2 の記録媒体に記録する記録手段と、

前記第 2 の記録媒体に記録された、前記暗号化された前記コピー禁止データを、前記鍵を利用して解読し、再生する再生手段とを備えた

ことを特徴とする記録再生装置。

70. 前記移動手段が前記データの移動を行ったさい、または前記複写手段が前記データの複写を行ったさい、前記データの移動または複写に対する課金情報を、前記データ処理装置を管理する管理装置に送信する課金情報送信手段をさらに備えたことを特徴とする請求項 45、46、47、48、49、50、51、52、59、60、61、62、63、64、65、66、67 のいずれかに記載のデータ処理装置。

71. 前記データ処理装置と前記他の記録装置とが接続されたインタフェースに、少なくとも前記コピー禁止データの移動または複写に対して課金

WO 01/48755

PCT/JP00/09260

147

能力を有する管理装置が接続されていることが確認されたときに、前記移動手段または前記複写手段は、前記コピー禁止データを前記他の記録装置に移動させるまたは複写することを特徴とする請求項 45、46、47、48、49、50、51、52、59、60、61、62、63、64、65、66、67 のいずれかに記載のデータ処理装置。

72. 同じ内容の、コピーが禁止されているコピー禁止データが暗号化されてそれぞれ記録されている複数の記録装置と、

それら複数の記録装置から出力される前記暗号化された前記コピー禁止データを復号する復号手段と、前記コピー禁止データと同じ内容であって、暗号化され、または暗号化されていないコピー禁止データを記録する記録手段とを有する復号記録装置とを備えた

ことを特徴とする暗号化データ復号記録装置システム。

73. 同じ内容の、コピーが禁止されているコピー禁止データが暗号化されてそれぞれ記録されている複数の記録装置から出力される前記暗号化された前記コピー禁止データを復号する復号手段と、

前記コピー禁止データと同じ内容であって、暗号化され、または暗号化されていないコピー禁止データを記録する記録手段とを備えた

ことを特徴とする復号記録装置。

74. 同じ内容の、コピーが禁止されているコピー禁止データが暗号化されてそれぞれ記録されている複数の記録装置のうちの一つの記録装置であって、

前記暗号化された前記コピー禁止データを記録する記録手段と、その記録手段に記録されている前記暗号化されたコピー禁止データを出力する出力手

WO 01/48755

PCT/JP00/09260

148

段とを備え、

その出力手段から出力される前記暗号化されたコピー禁止データは、その暗号化されたコピー禁止データを復号する復号手段を少なくとも有する復号記録装置においてのみ復号されるデータである

ことを特徴とする記録装置。

75. 複数のデータで構成されているストリームを送信する送信手段を備え、

前記ストリームの、または前記ストリームを構成する各ブロック内の、複数の前記データそれぞれは、そのデータの時間上一つ手前のデータが再生されないと再生されないデータであって、

前記送信手段は、前記ストリームの、または前記ストリームを構成する各ブロック内の、前記複数のデータの時間的に最後尾から先頭側の順に、前記各データを送信する

ことを特徴とするデータ送信装置。

76. 複製が禁止または制限されるよう設定されているデータからなる複製制限コンテンツをタイムシフト再生可能にするための記録装置であって、

所定の容量分、前記複製制限コンテンツの記録が可能な記録媒体と、

前記記録媒体に対しデータの記録を行う記録手段とを備え、

前記記録手段は、前記複製制限コンテンツを前記記録媒体に記録するとともに、前記複製制限コンテンツの記録を開始した時刻から、所定の時間が経過した後、前記記録媒体に記録された前記複製制限コンテンツのデータを、視聴することが不可能な状態にすることを特徴とする記録装置。

WO 01/48755

PCT/JP00/09260

149

77. 前記視聴することが不可能な状態を、前記複製制限コンテンツのデータを消去することにより実現することを特徴とする請求項76記載の記録装置。

78. 前記視聴することが不可能な状態を、前記複製制限コンテンツのデータを消去しないことにより実現することを特徴とする請求項76記載の記録装置。

79. 前記視聴することが不可能な状態を、前記複製制限コンテンツのデータを再生不可能にすることにより実現することを特徴とする請求項76記載の記録装置。

80. 前記視聴することが不可能な状態を、再生後の前記複製制限コンテンツのデータを暗号化することにより実現することを特徴とする請求項79記載の記録装置。

81. 前記記録手段が、前記複製制限コンテンツの記録を開始するタイミングは、前記複製制限コンテンツに関連した判別情報を参照することにより定められることを特徴とする請求項76～80のいずれかに記載の記録装置。

82. 前記記録手段は、前記判別情報を用いて、前記複製制限コンテンツと他のコンテンツとを分別して記録を行うことを特徴とする請求項81記載の記録装置。

83. 前記判別情報は、前記複製制限コンテンツのデータ列に含まれる著作権情報であることを特徴とする請求項81記載の記録装置。

84. 前記記録手段が、前記複製制限コンテンツの記録を開始するタイミングは、外部からの入力に基づき定められることを特徴とする請求項76

WO 01/48755

PCT/JP00/09260

150

～ 8 2 のいずれかに記載の記録装置。

8 5. 前記記録媒体は、前記複製制限コンテンツの一時記録を行うための記録バッファを有することを特徴とする請求項 7 6 ～ 8 0 のいずれかに記載の記録装置。

8 6. 前記記録用バッファは、同一領域に上書き記録を繰り返すことにより一定量のデータを記録することが可能なリングバッファであることを特徴とする請求項 8 5 記載の記録装置。

8 7. 請求項 7 6 ～ 8 5 のいずれかに記載の記録装置と、
前記記録媒体に記録されたデータを再生する再生手段とを備えた記録再生装置であって、

前記再生手段は、前記複製制限コンテンツが記録開始された時刻から、所定の待機時間が経過した後、記録された前記複製制限コンテンツを再生することを特徴とする記録再生装置。

8 8. 請求項 8 6 記載の記録装置と、
前記記録媒体に記録されたデータを再生する再生手段とを備えた記録再生装置であって、

前記再生手段は、前記複製制限コンテンツが記録開始された時刻から、所定の待機時間が経過した後、記録された前記複製制限コンテンツを再生することを特徴とする記録再生装置。

8 9. 前記リングバッファに上書き記録が行われている状態で、前記再生手段が再生動作を行う際は、前記リングバッファ上にて、最も古いデータが記録されている位置から該データの再生を行うことを特徴とする請求項 8 8 記載の記録再生装置。

WO 01/48755

PCT/JP00/09260

151

90. 前記リングバッファに上書き記録が行われていない状態で、前記再生手段が再生動作を行う際は、前記リングバッファ上の記録開始位置から前記データの再生を行うことを特徴とする請求項89記載の記録再生装置。

91. 前記記録装置は、前記記録媒体に記録された複製制限コンテンツが、前記所定の待機時間内に再生されない場合、該複製制限コンテンツの記録動作を停止することを特徴とする請求項87または88に記載の記録再生装置。

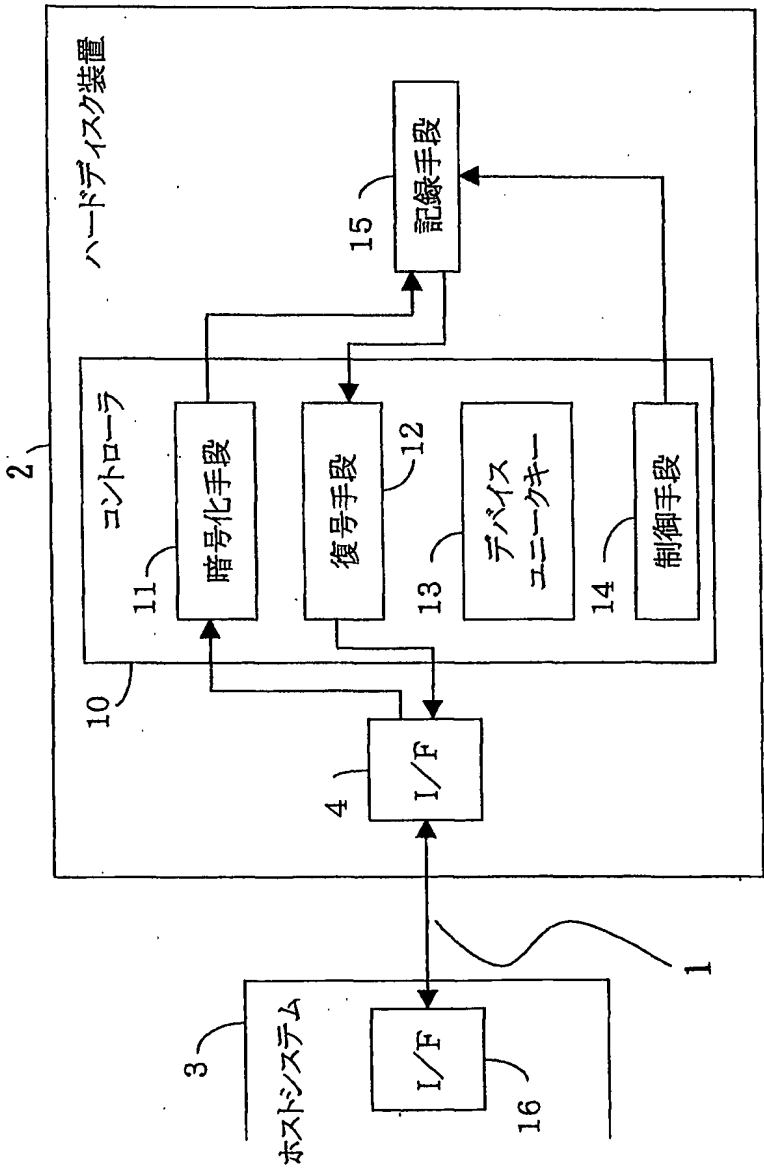
92. 前記所定の時間または前記所定の待機時間のいずれかに基づき、前記記録装置または再生手段の動作内容をあらかじめ告知する告知手段をさらに備えたことを特徴とする請求項87または88に記載の記録再生装置。

93. 前記記録手段は、前記所定の時間を含む時間情報を、計測できることを特徴とする請求項76記載の記録装置。

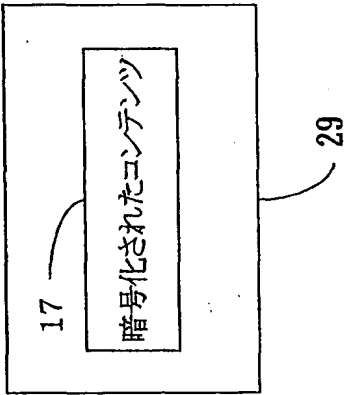
94. 前記複製制限コンテンツは、前記所定の時間を含む時間情報を含んでいることを特徴とする請求項76記載の記録装置。

95. 前記所定の時間を含む時間情報を、前記複製制限コンテンツとは独立して外部から取得することを特徴とする請求項76記載の記録装置。

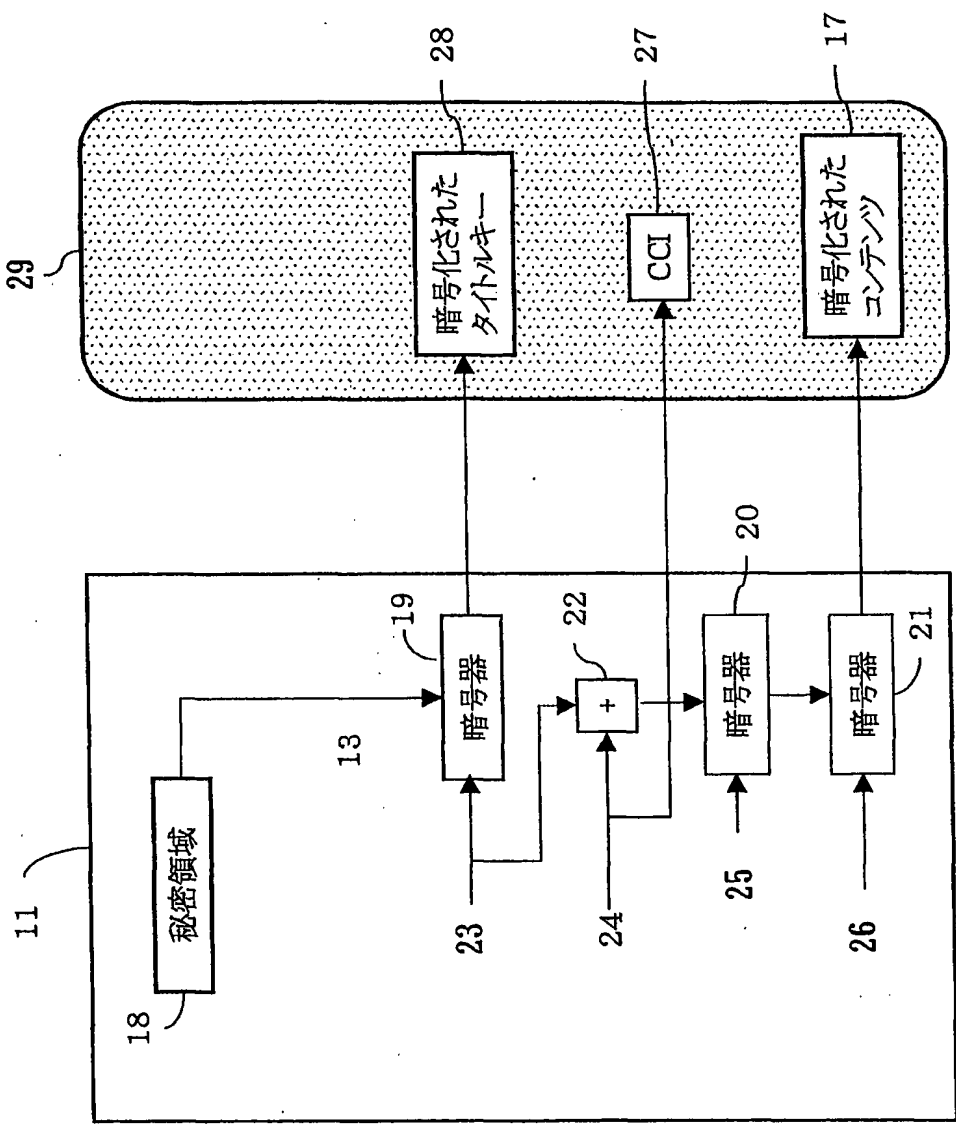
第1図



第2図



第3図

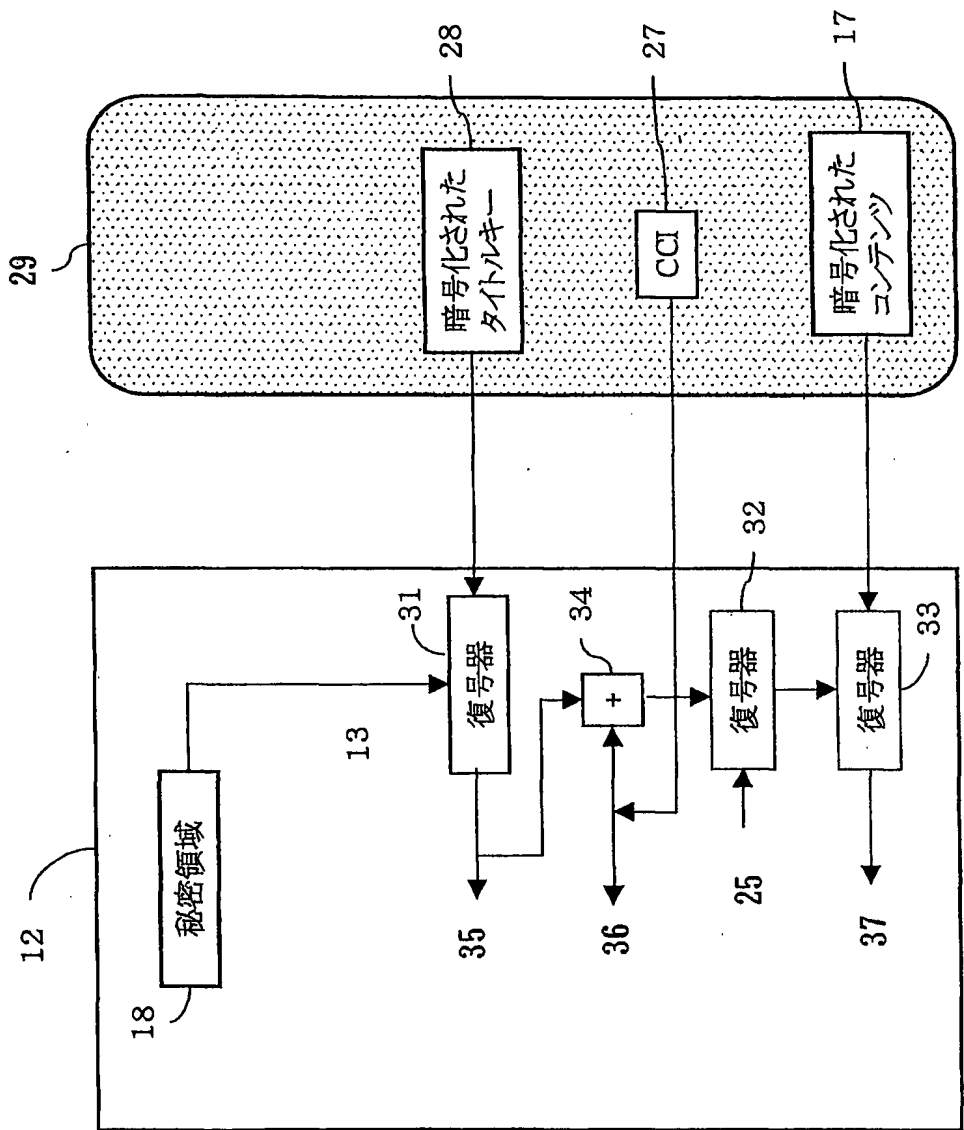


WO 01/48755

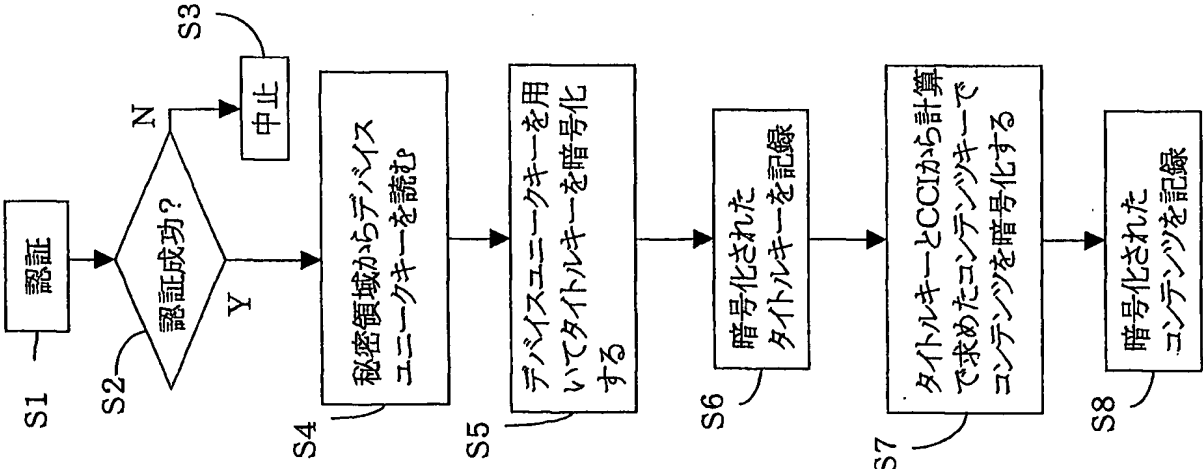
PCT/JP00/09260

3/39

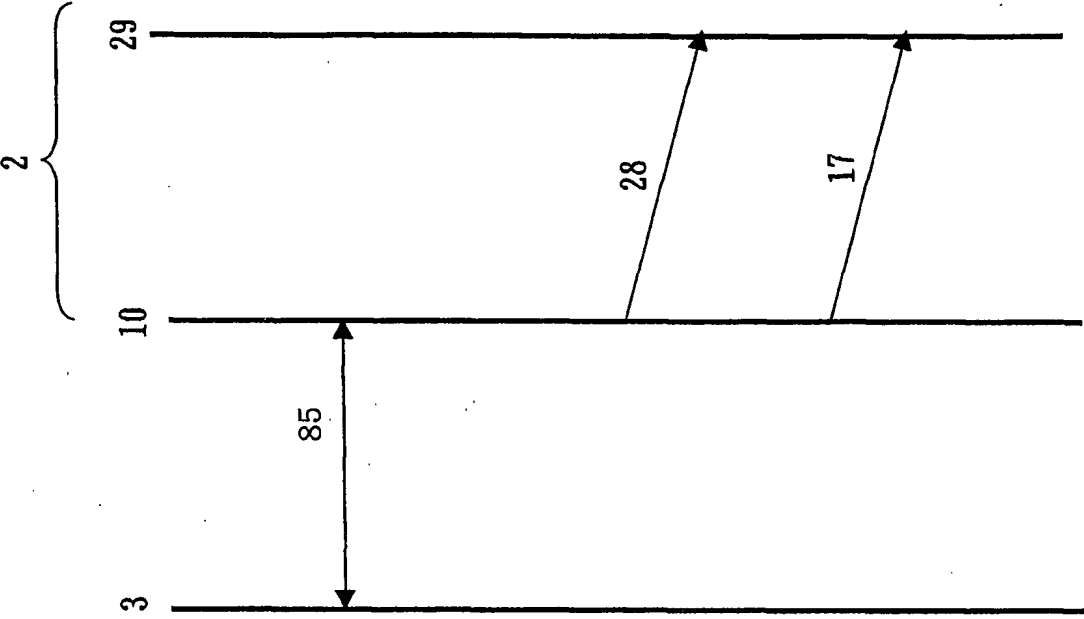
第4図



第5 (a) 図

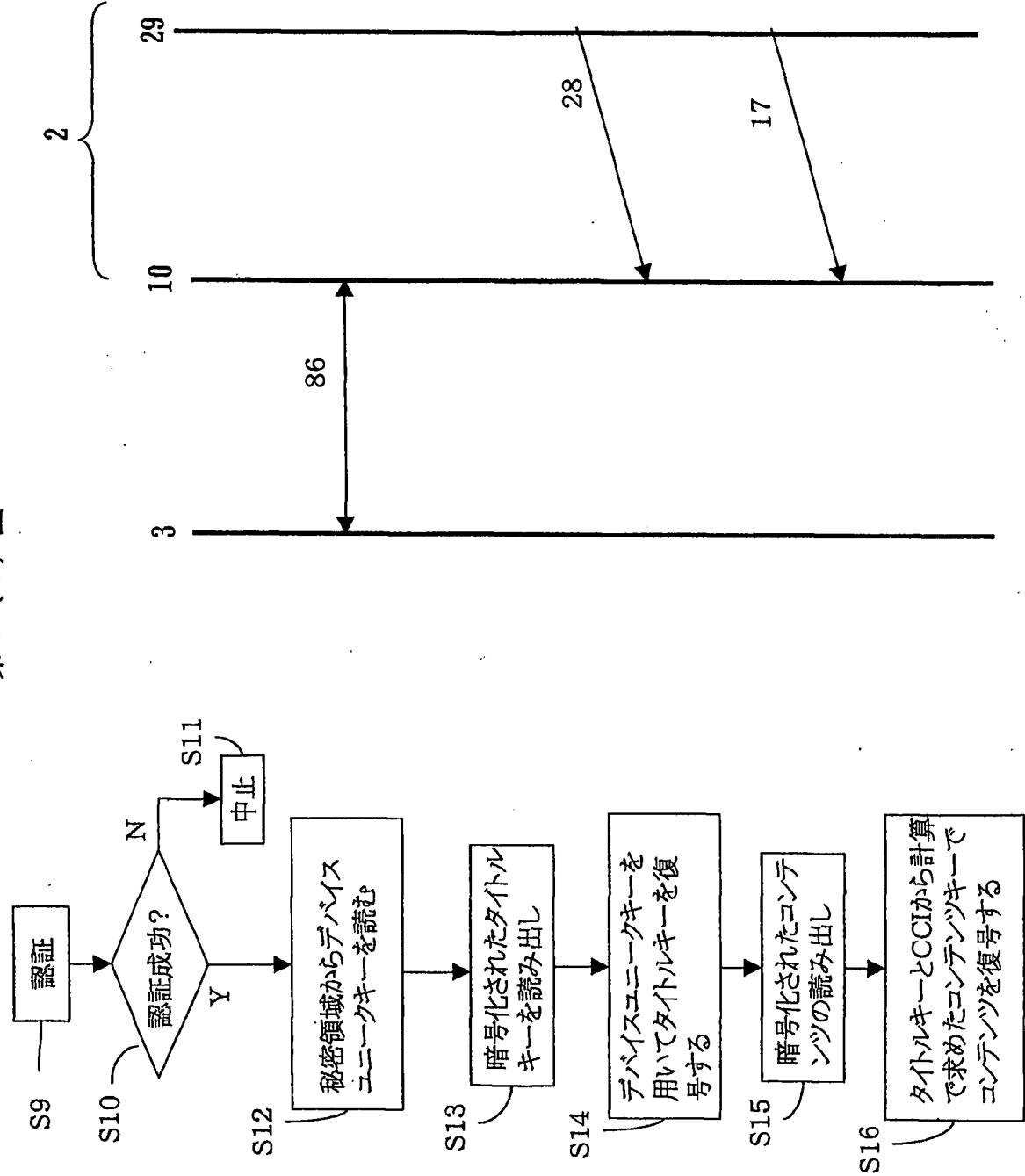


第5 (b) 図

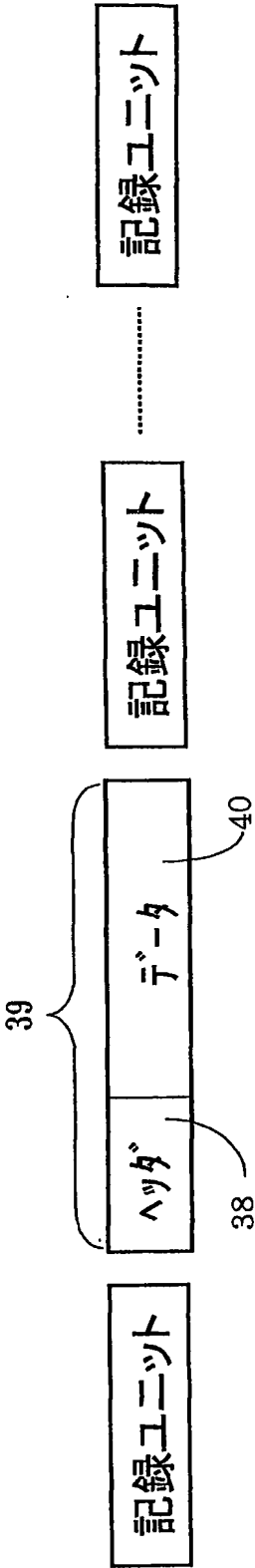


第6 (a) 図

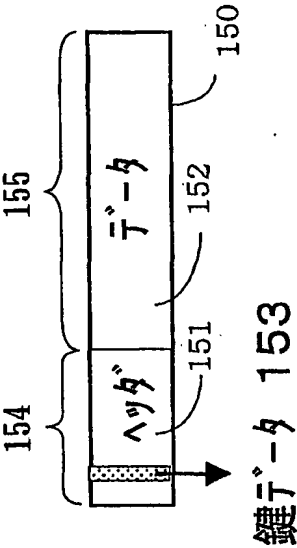
第6 (b) 図



第7 (a) 図



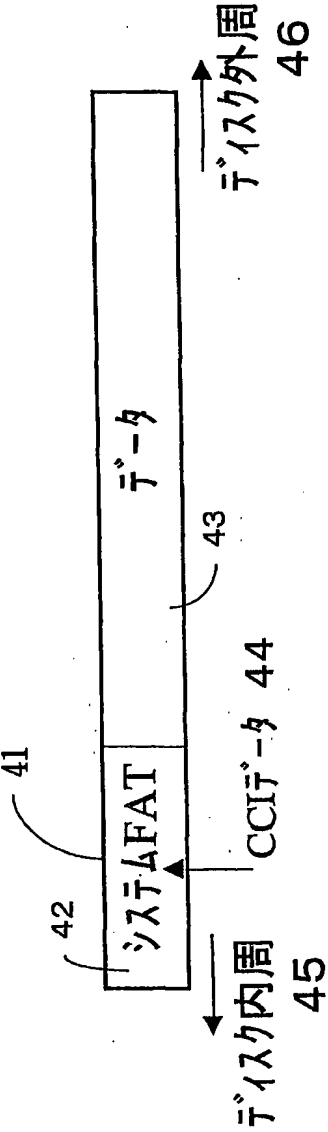
第7 (b) 図



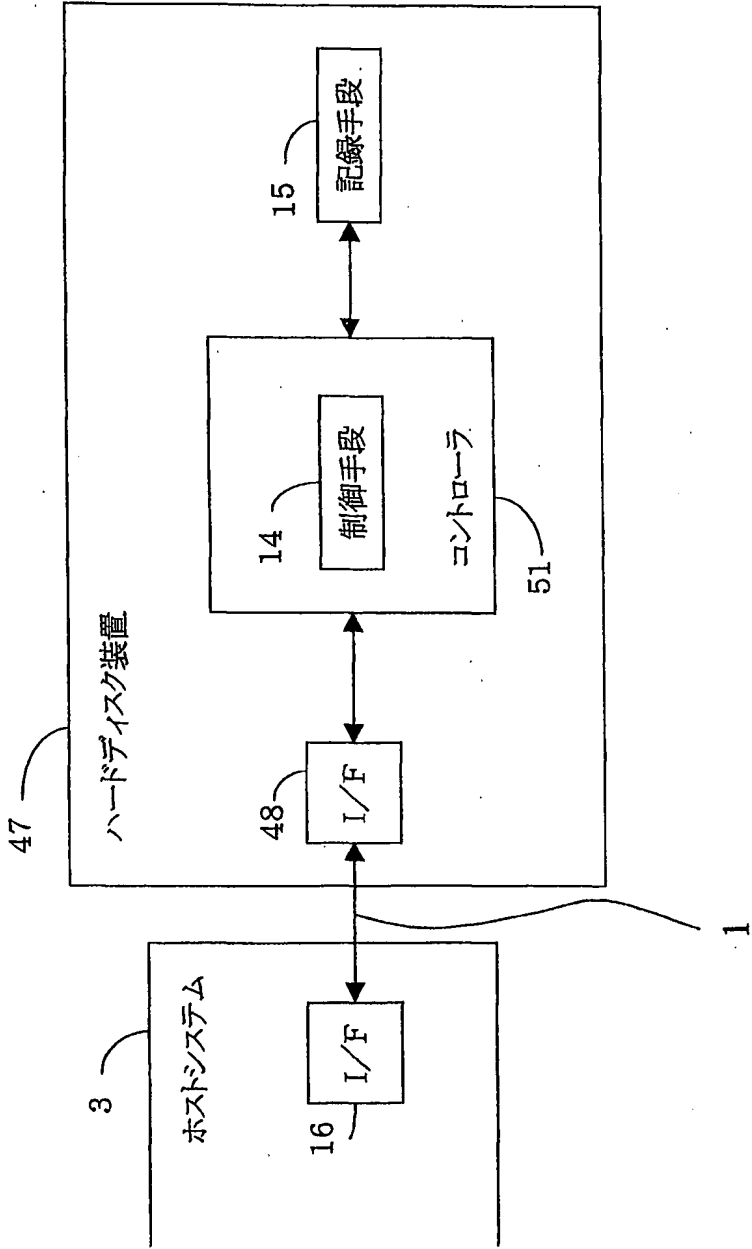
第8図

CCIの値	意味
11	Copy Never
10	Copy Once
01	No More Copy
00	Copy Free

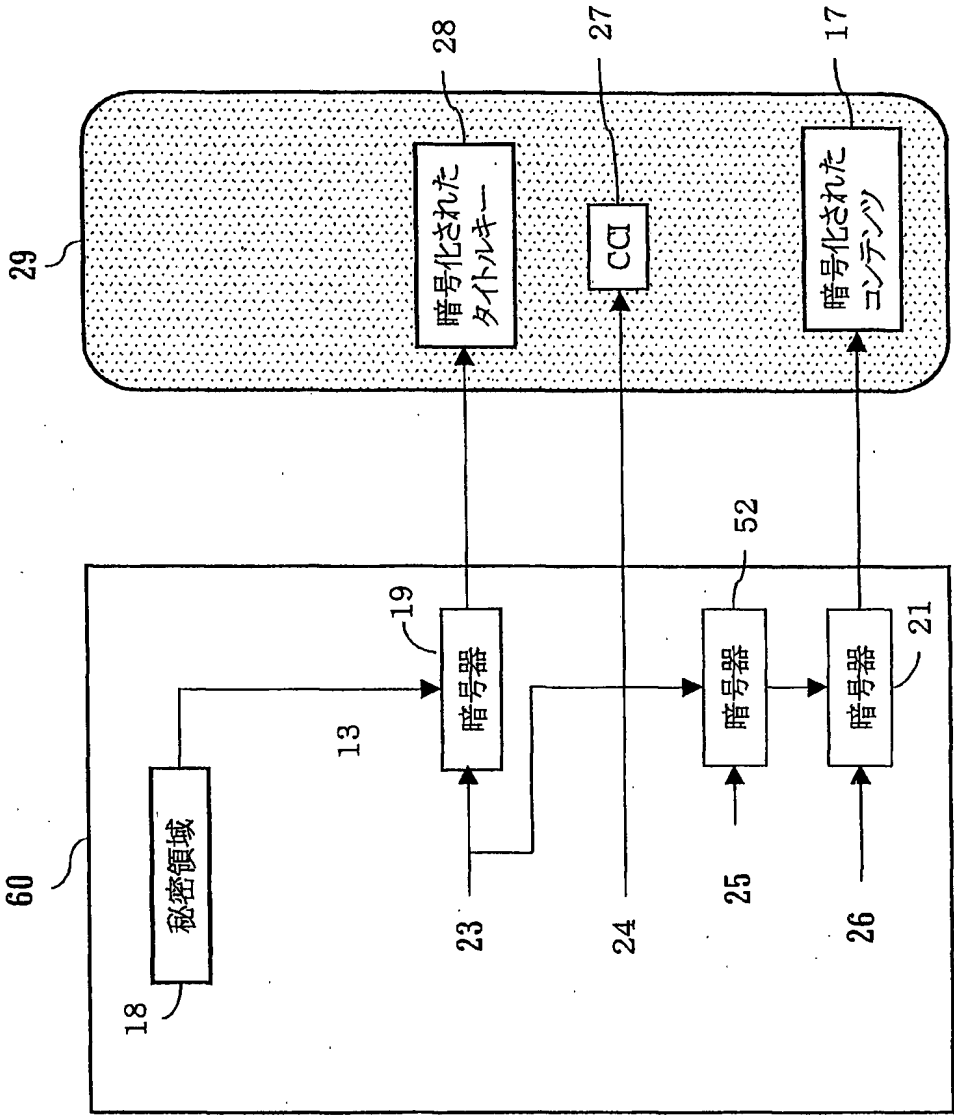
第9図



第10図



第11図

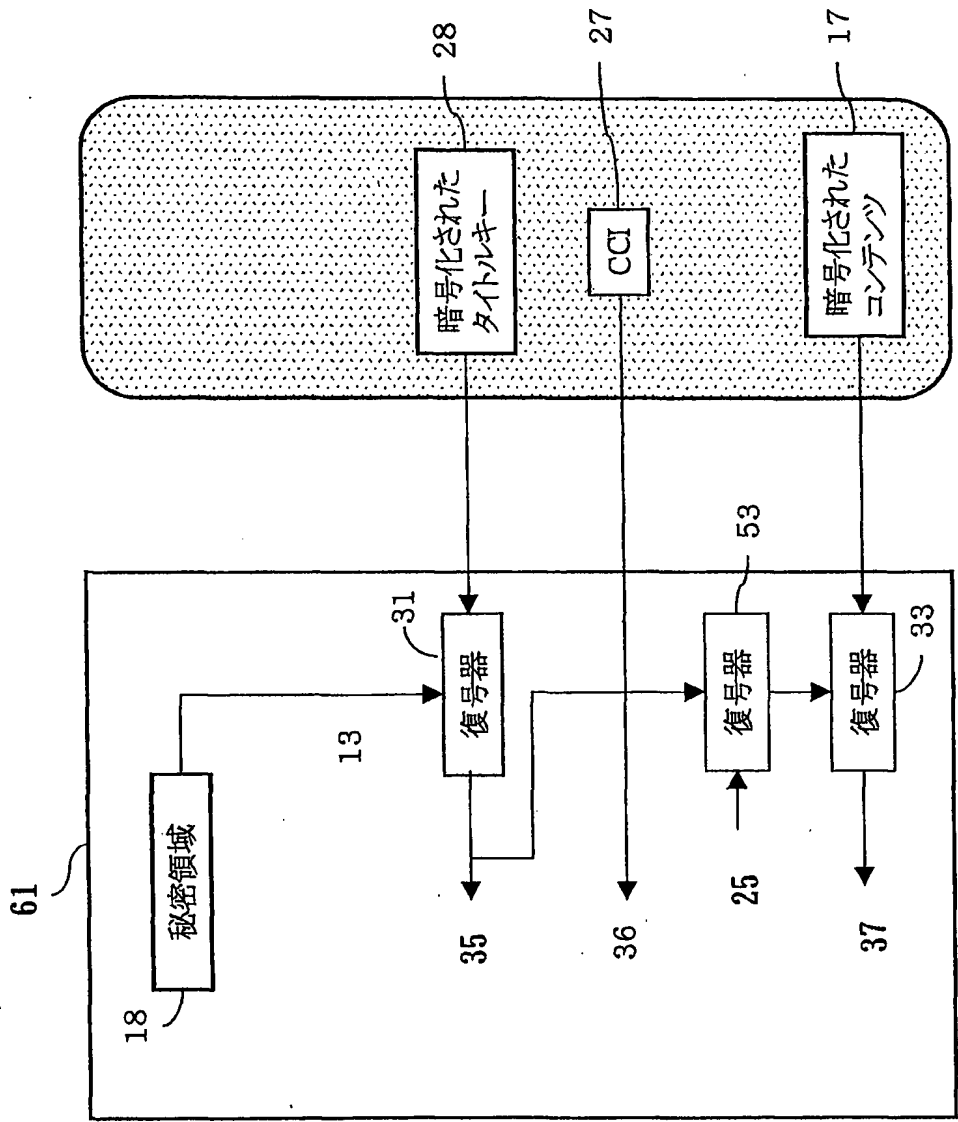


WO 01/48755

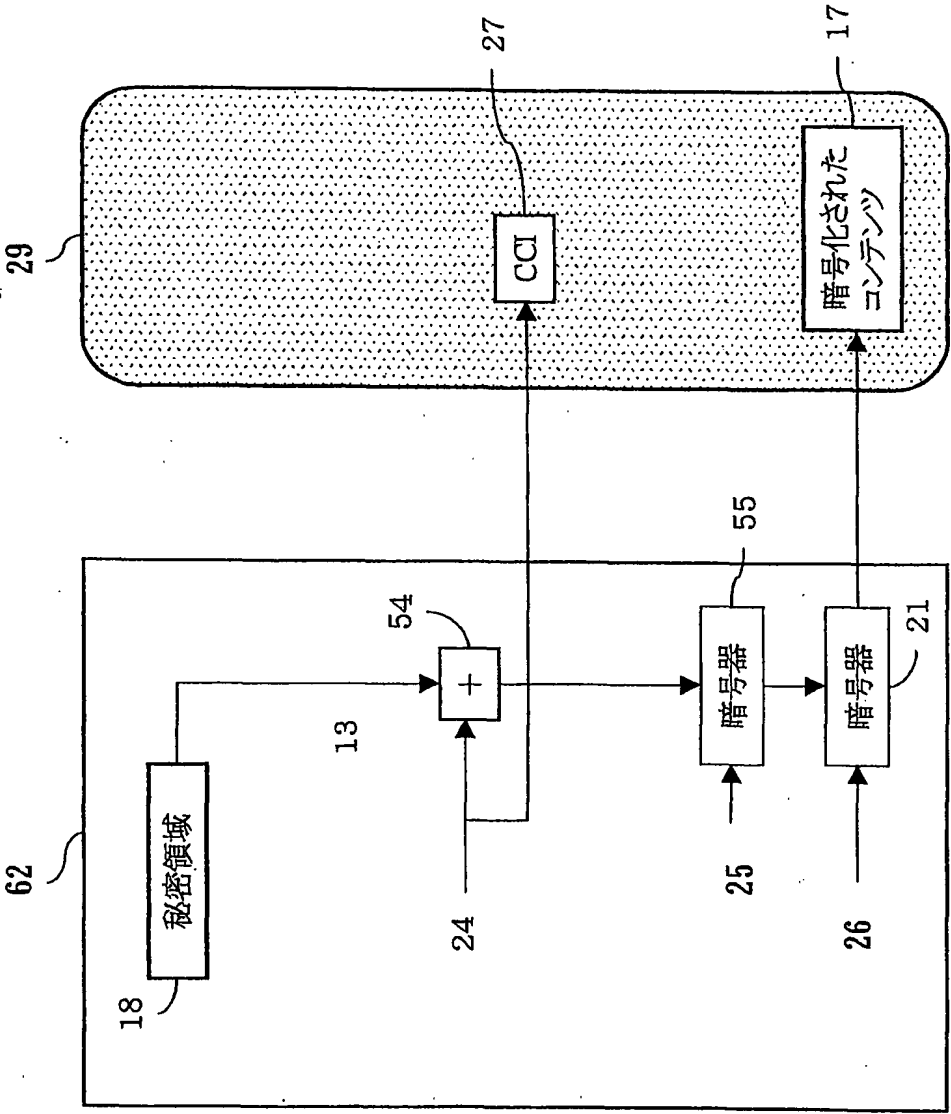
PCT/JP00/09260

10/39

第12図



第13図

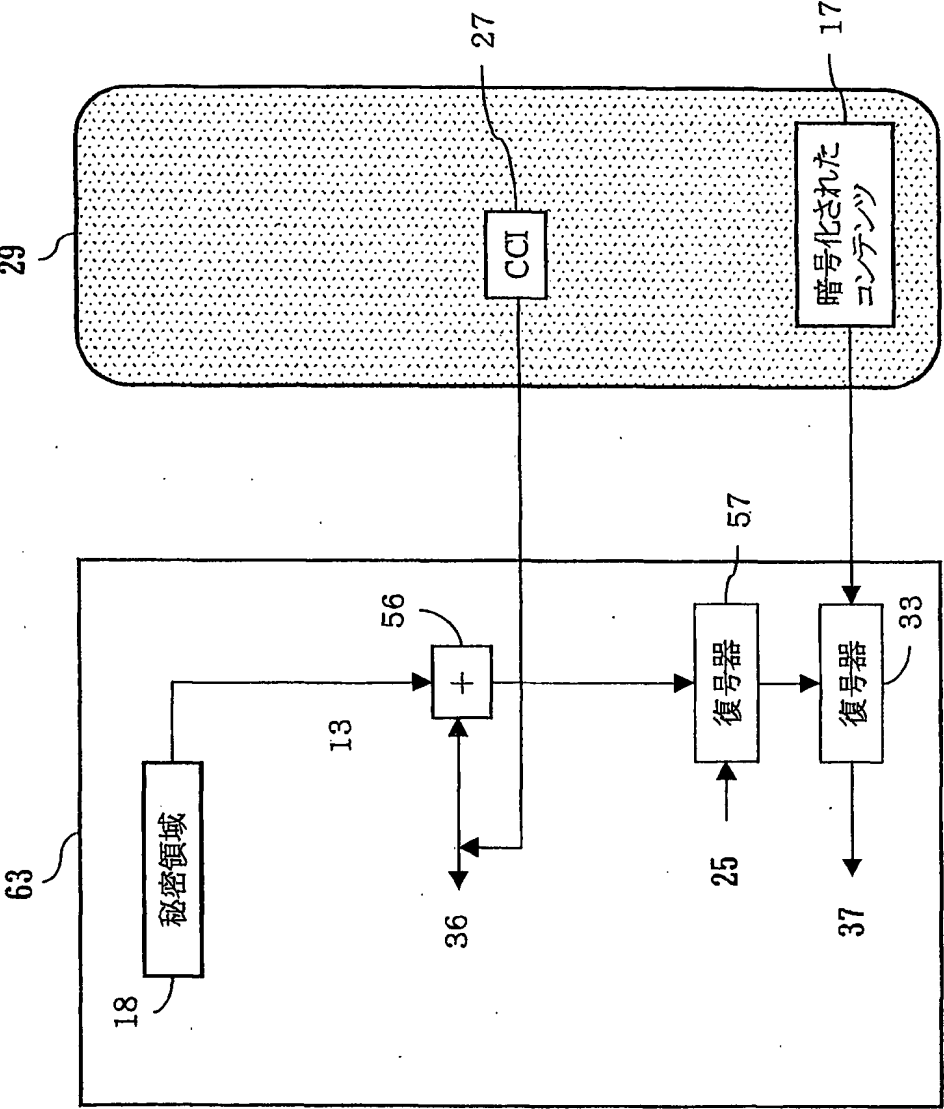


WO 01/48755

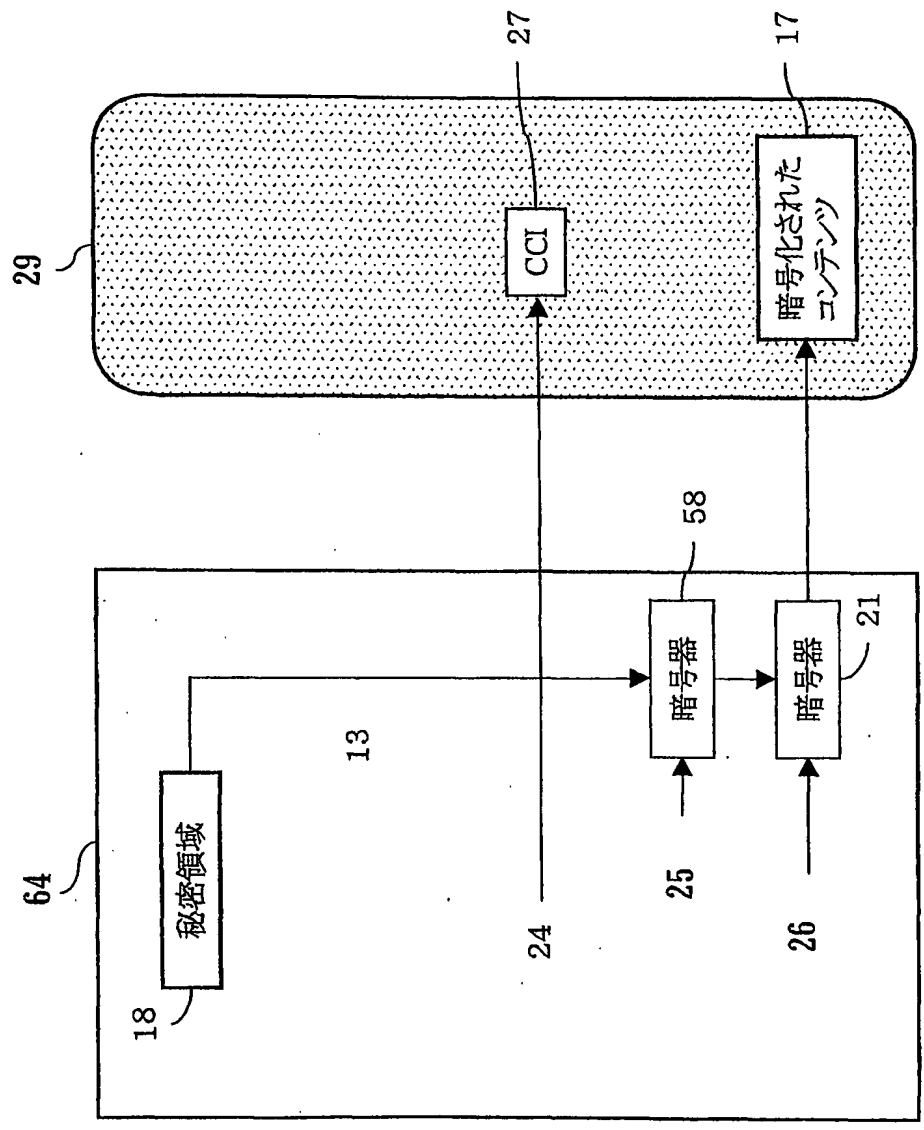
PCT/JP00/09260

12/39

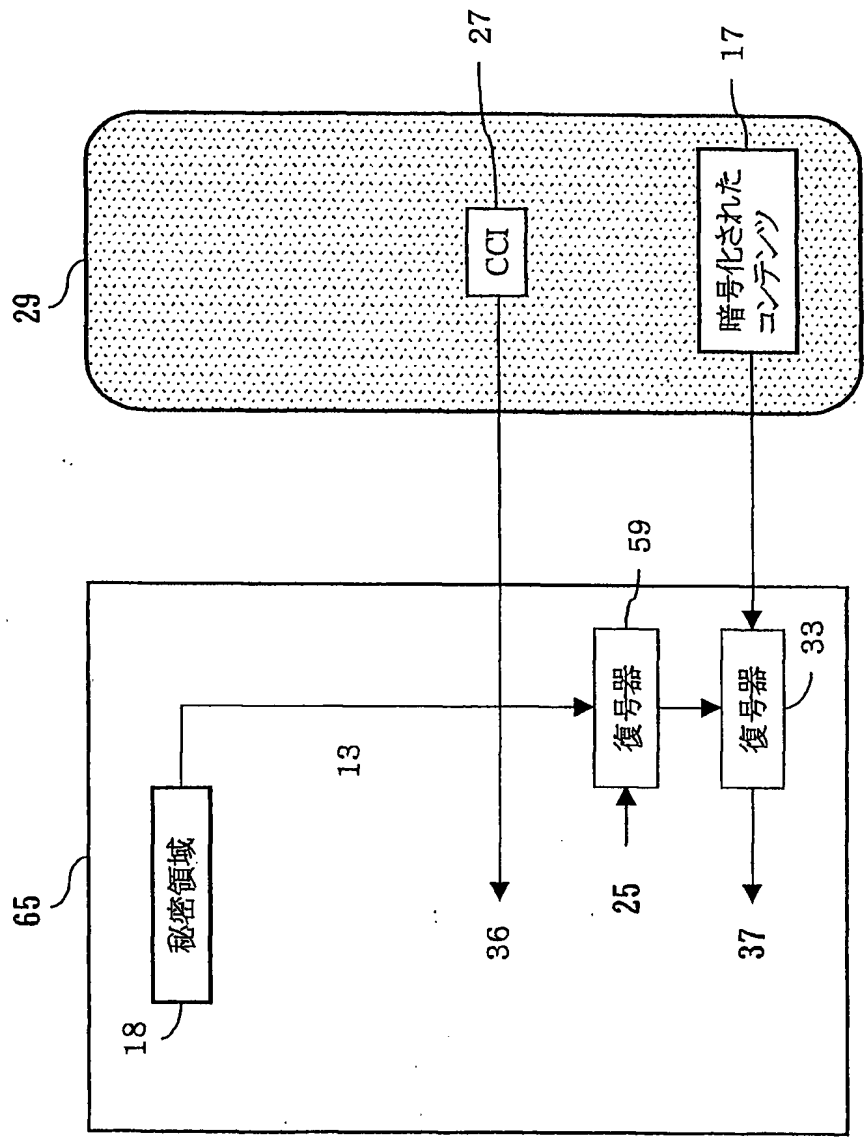
第14図



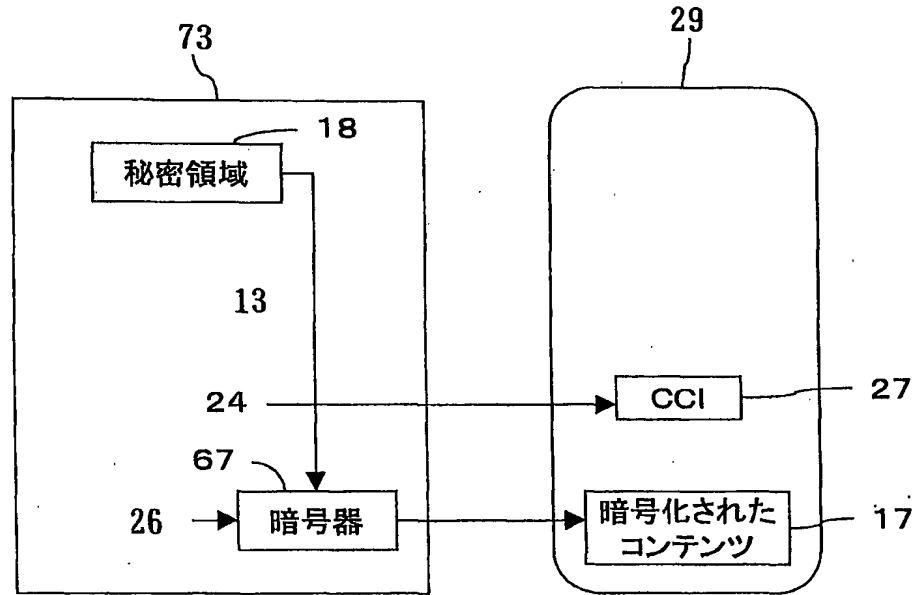
第15図



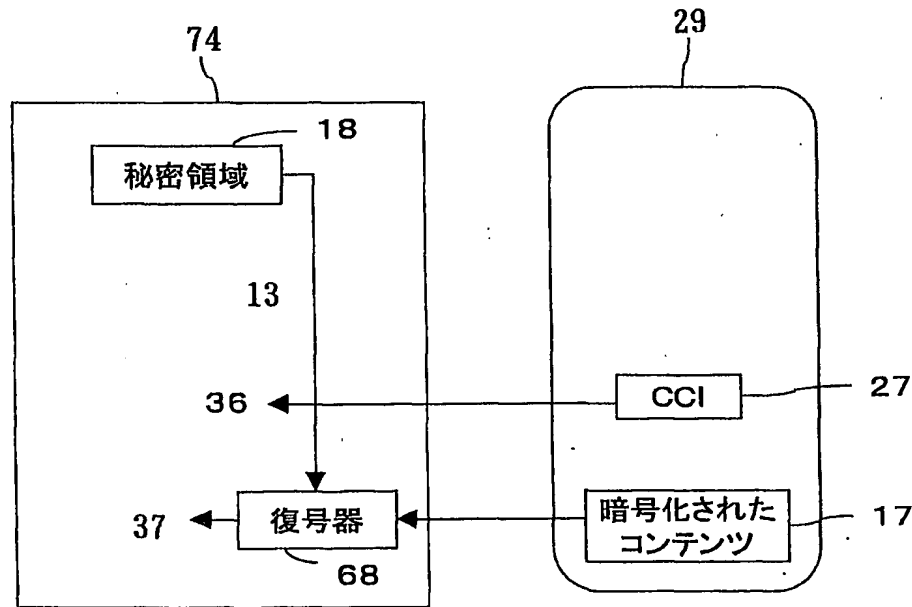
第16図



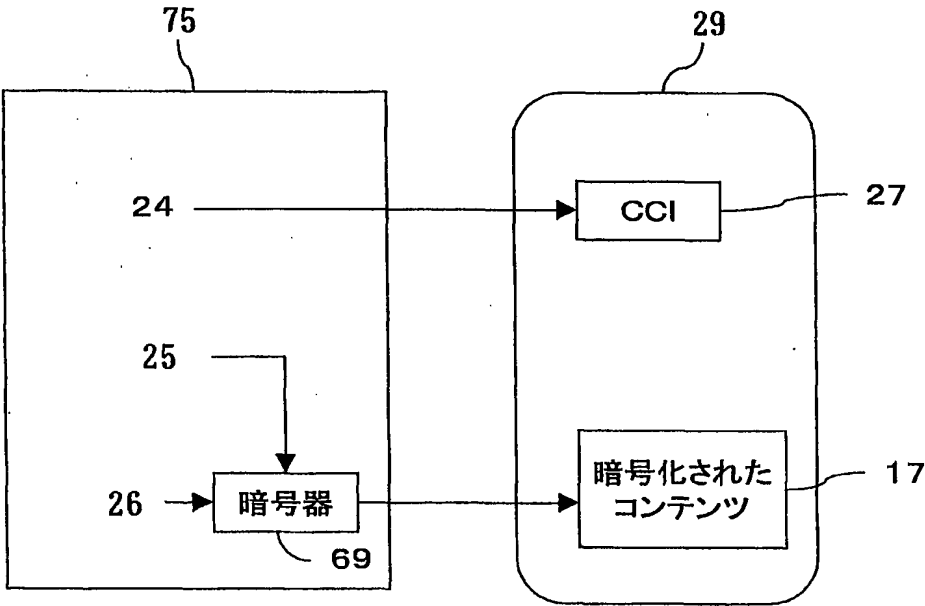
第17 (a) 図



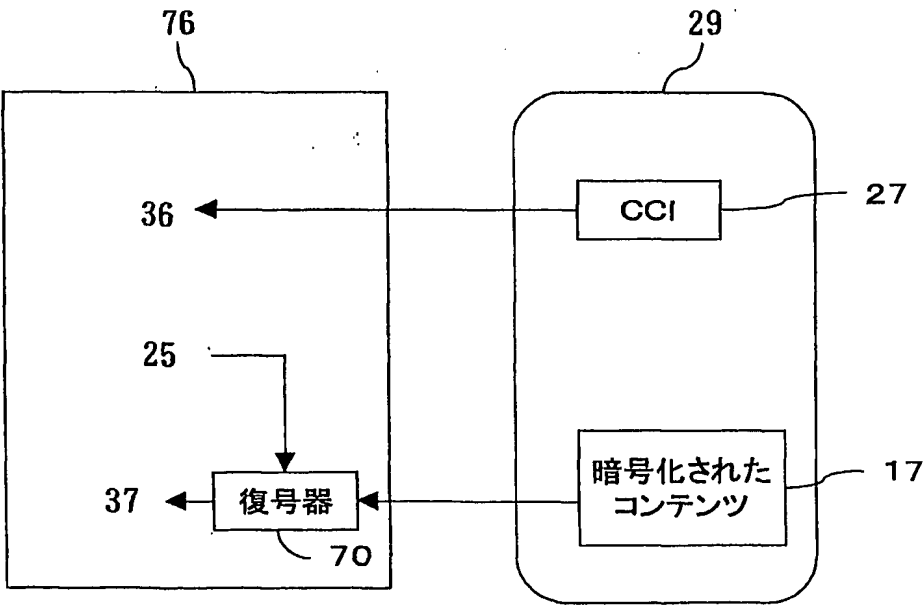
第17 (b) 図



第18 (a) 図

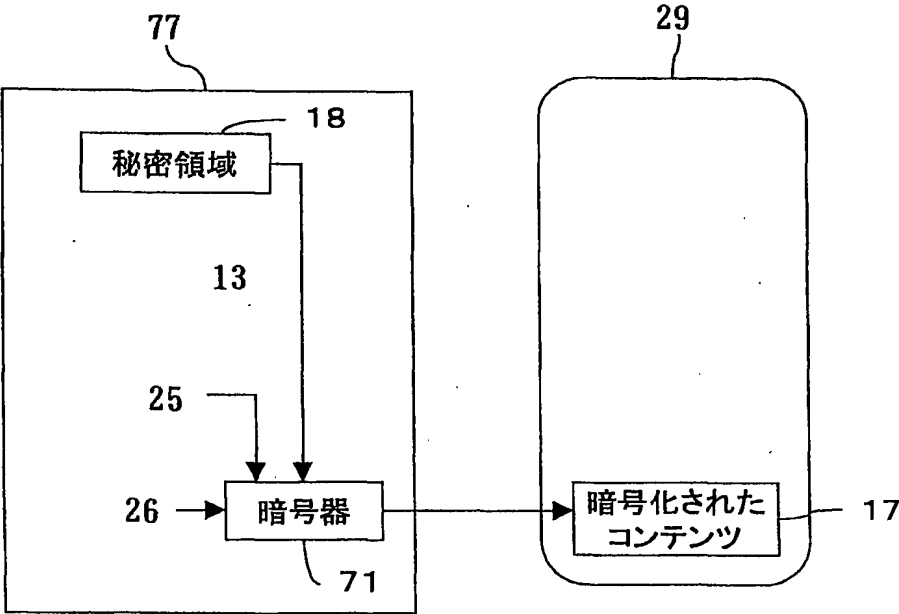


第18 (b) 図

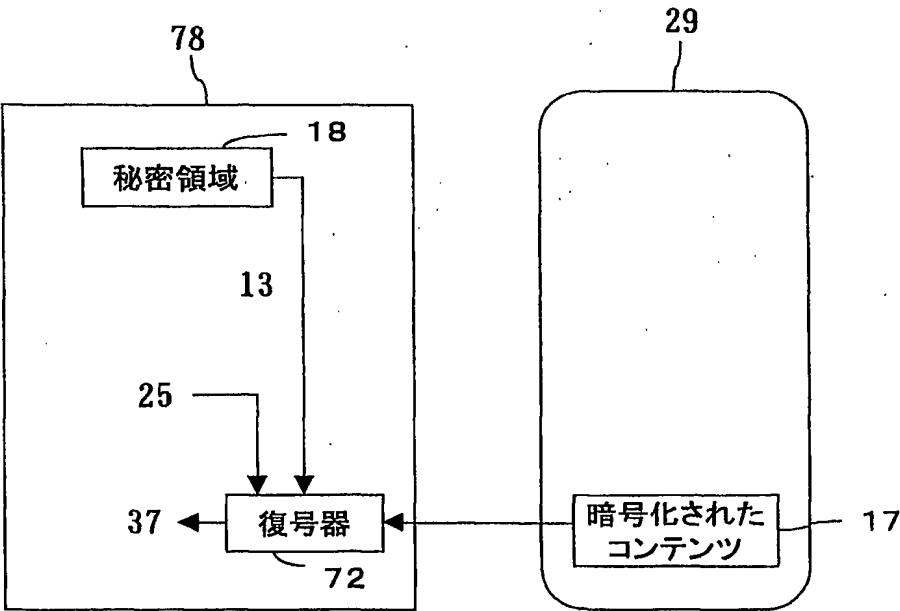


17/39

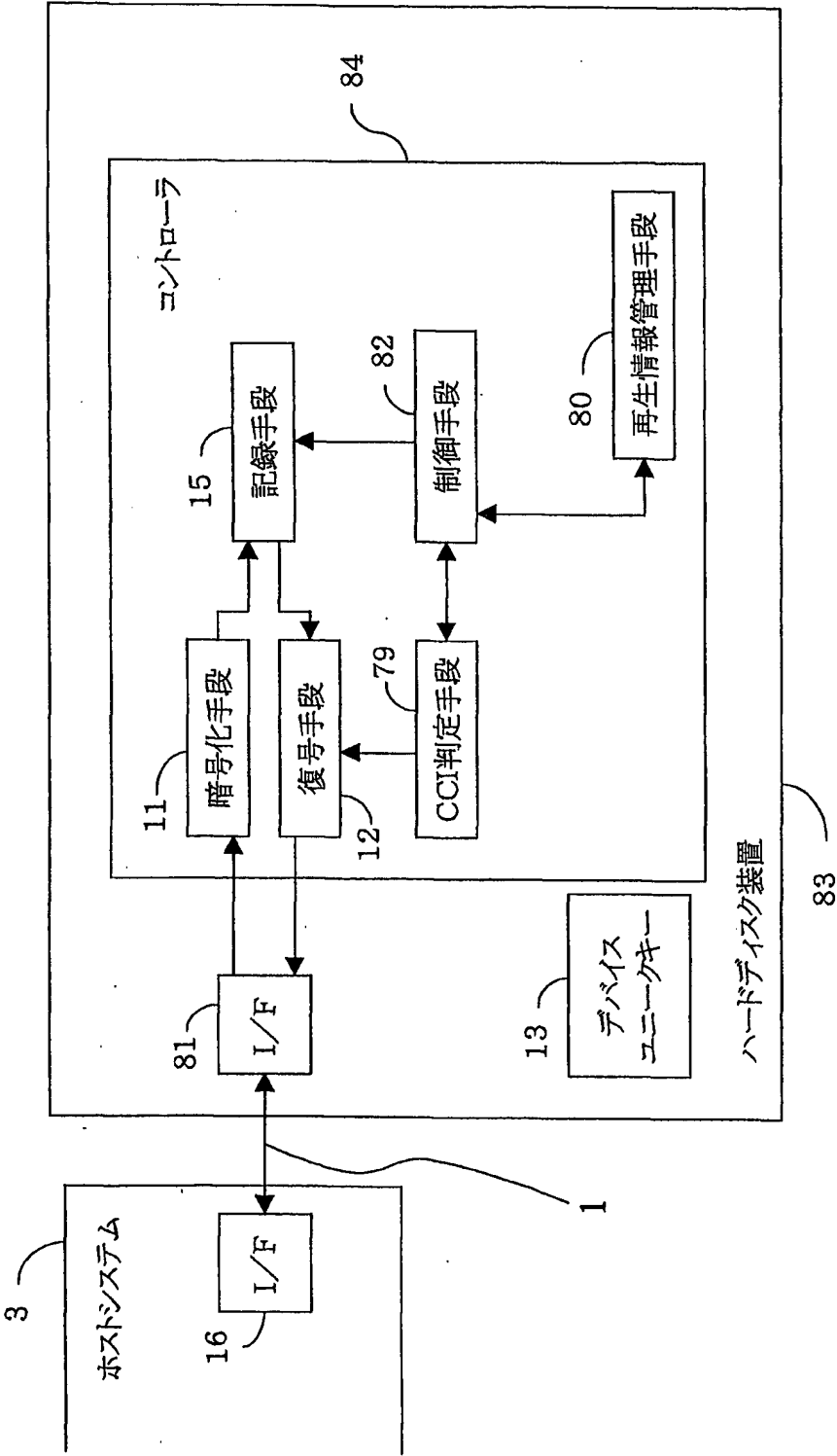
第 19 (a) 図



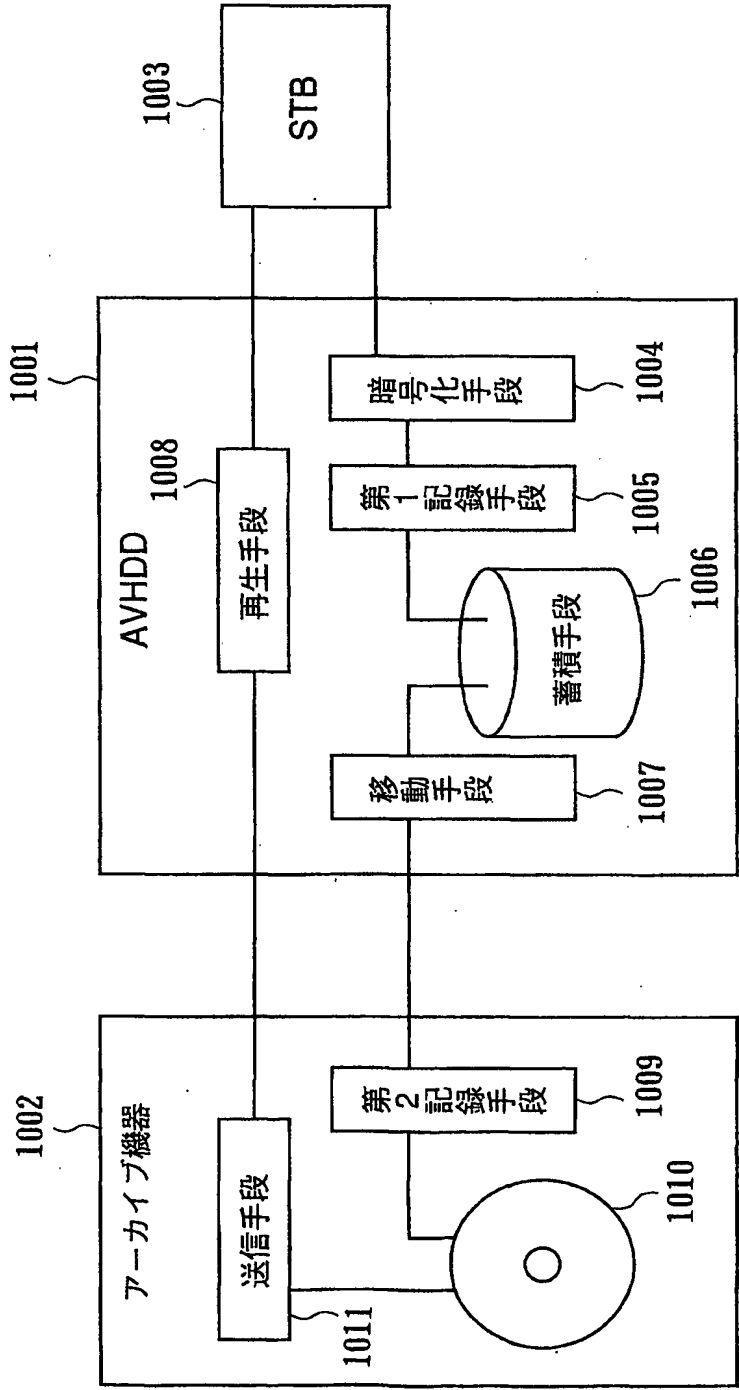
第 19 (b) 図



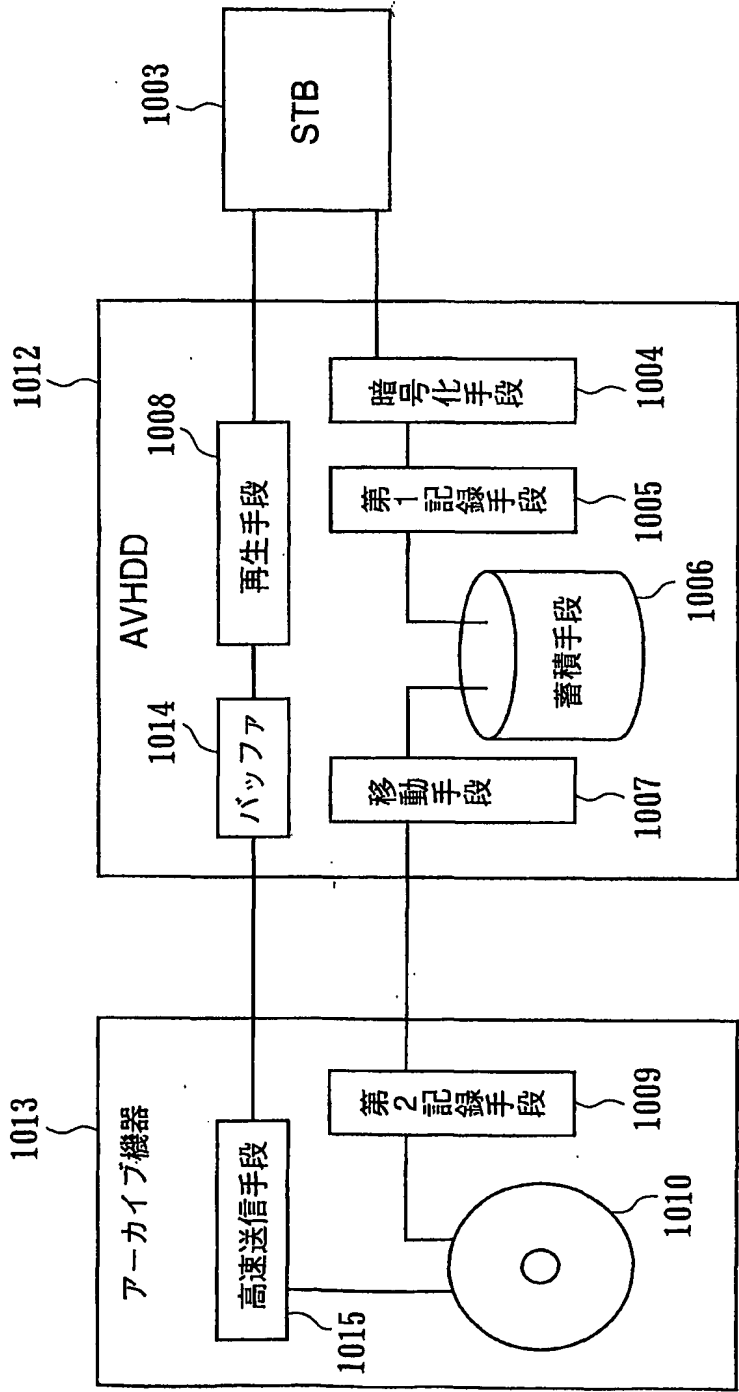
第20図



第21図



第22図

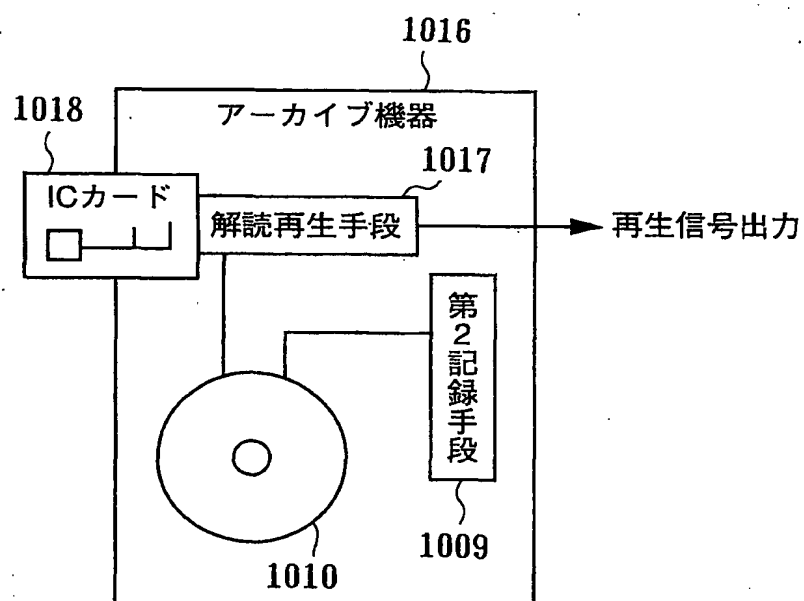


WO 01/48755

PCT/JP00/09260

21/39

第23図

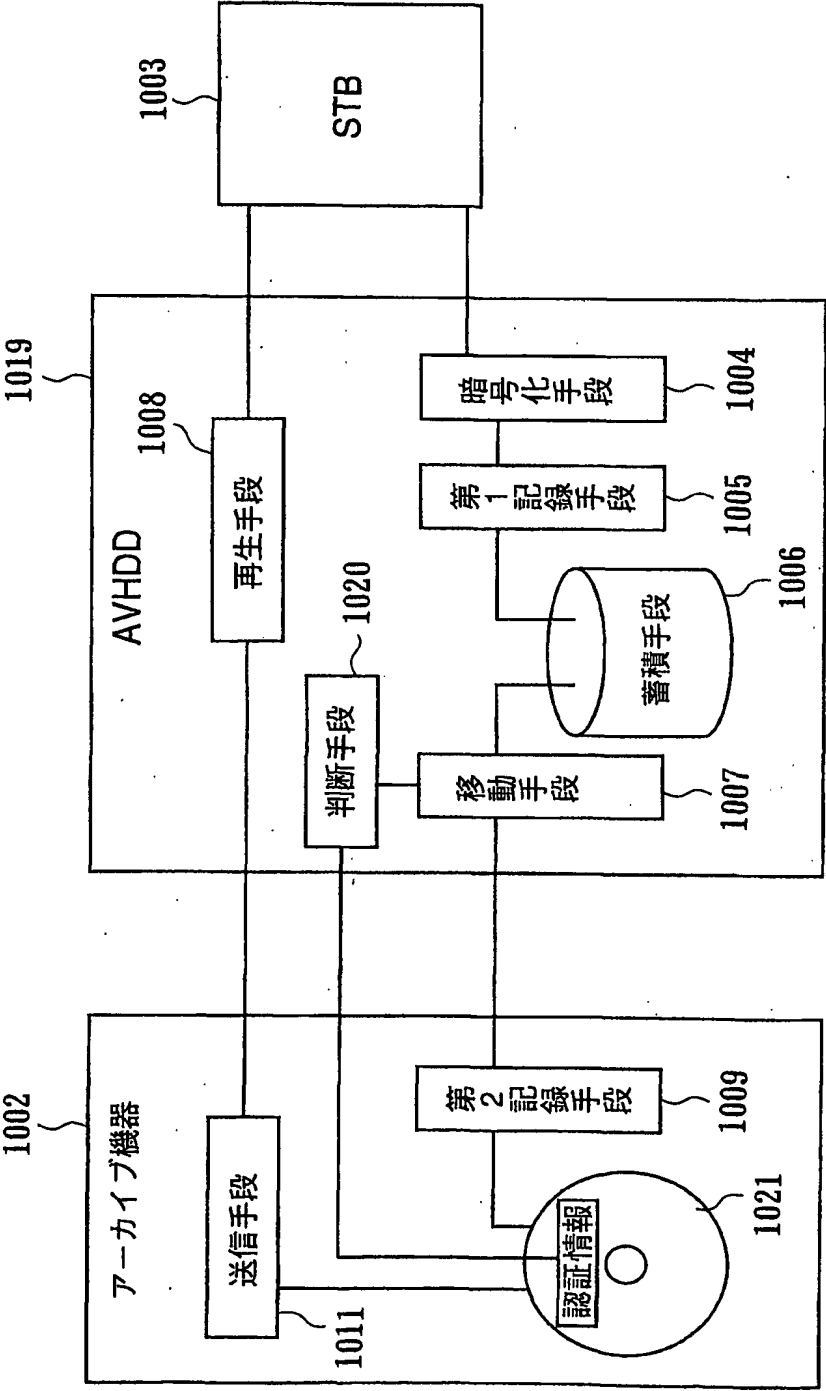


WO 01/48755

PCT/JP00/09260

22/39

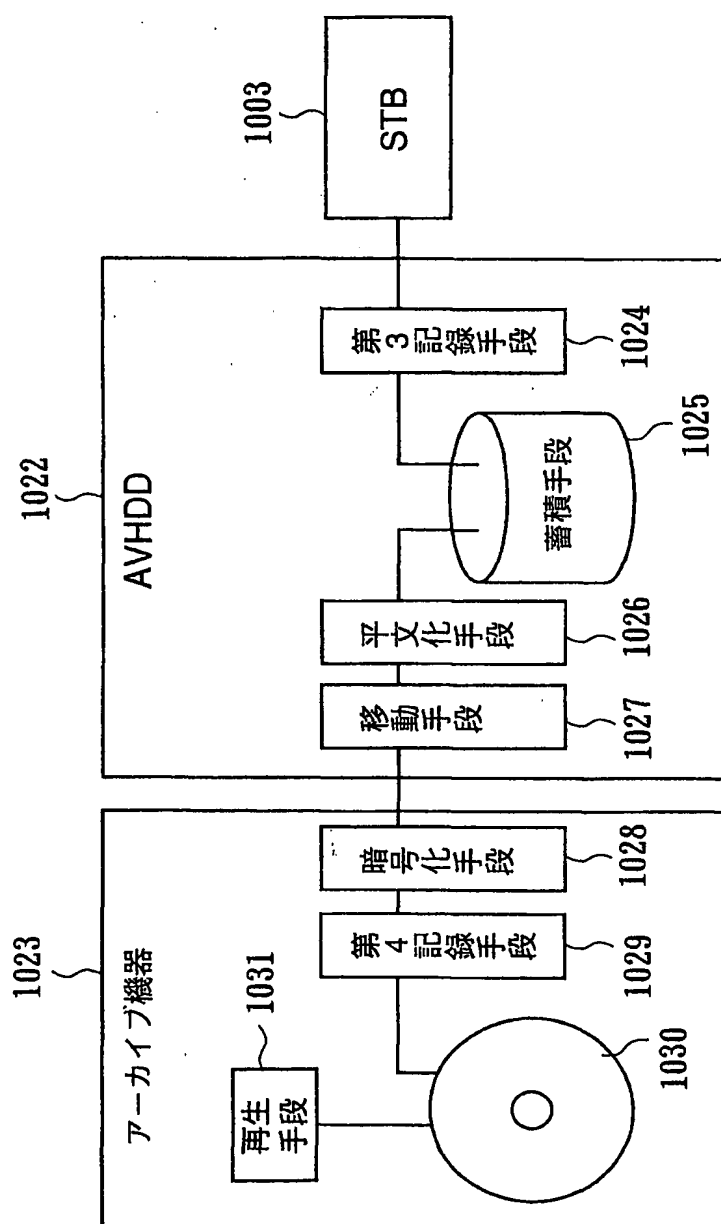
第24図



WO 01/48755

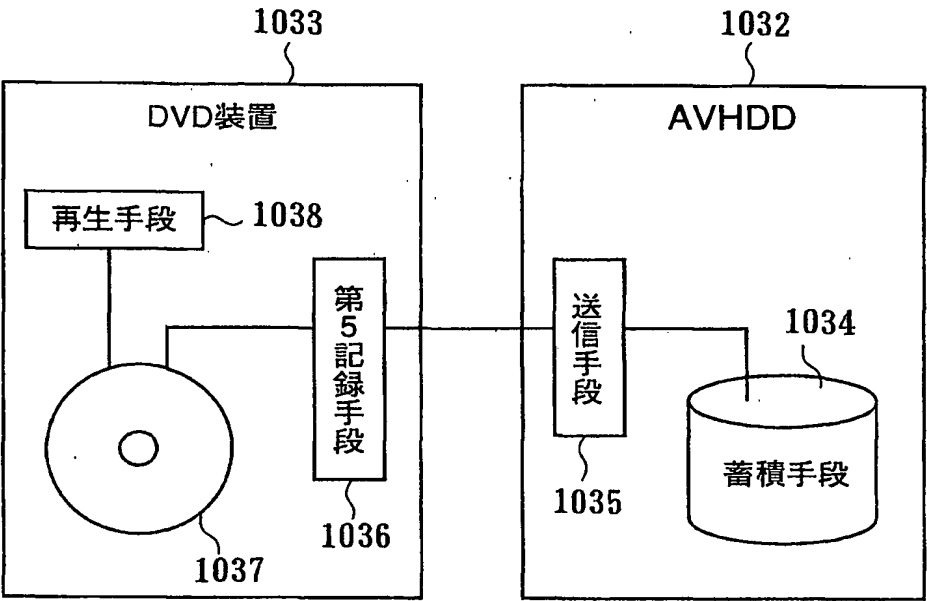
PCT/JP00/09260

23/39

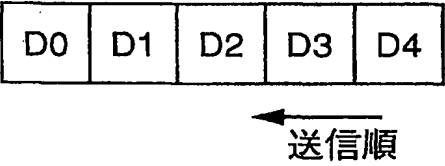


第25図

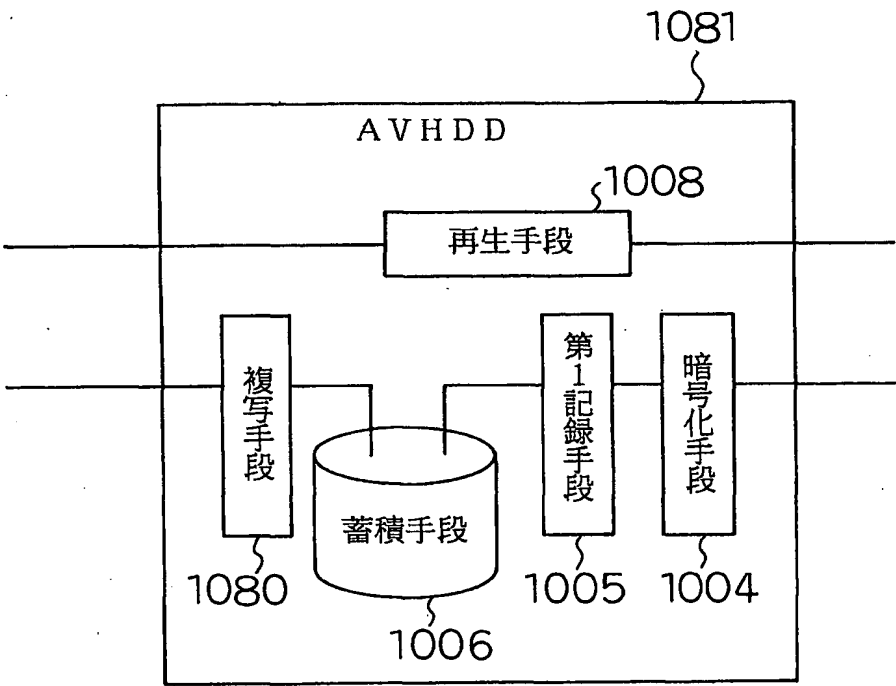
第 2 6 図



第 2 7 図



第 2 8 図

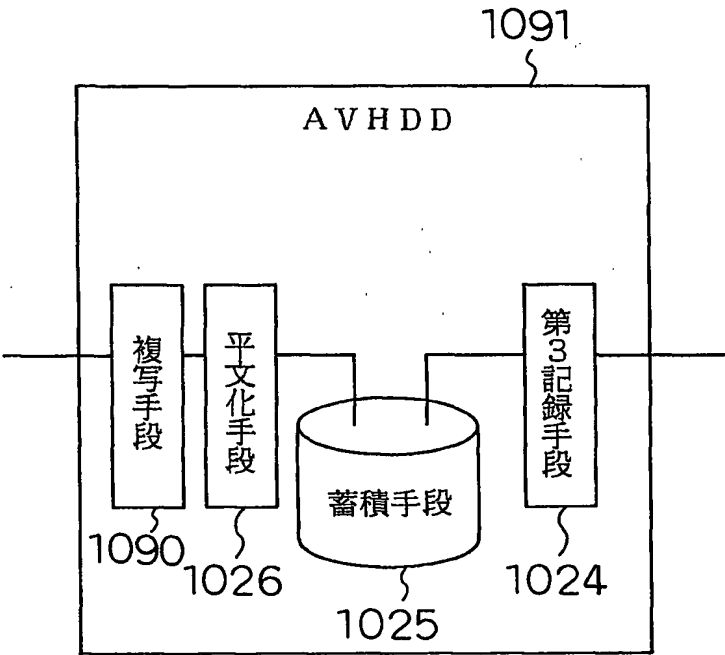


WO 01/48755

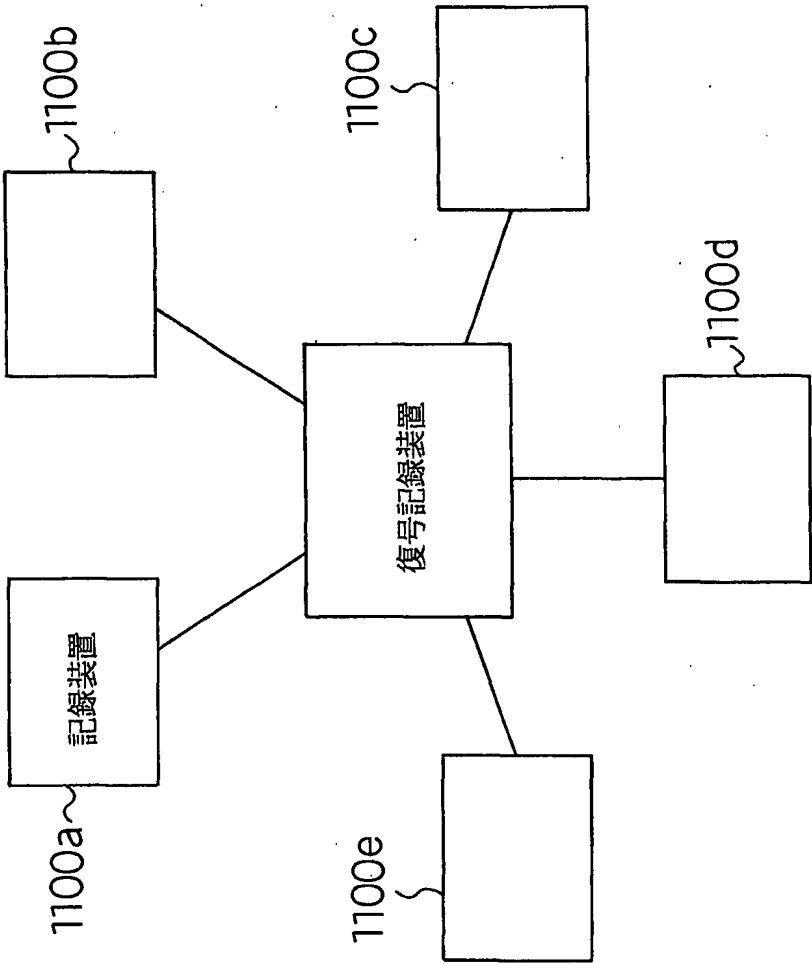
PCT/JP00/09260

26/39

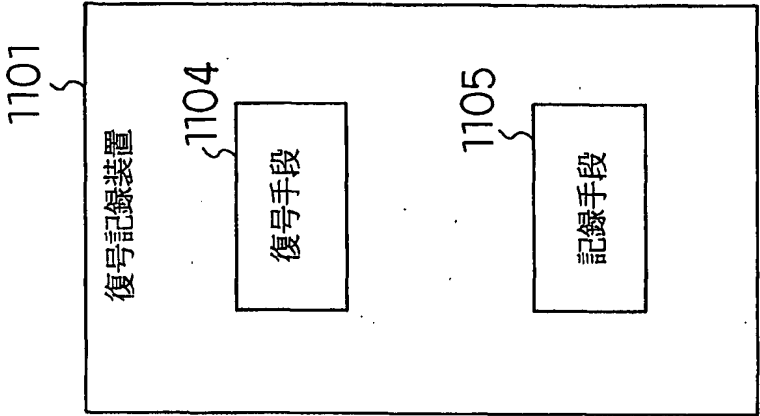
第 2 9 図



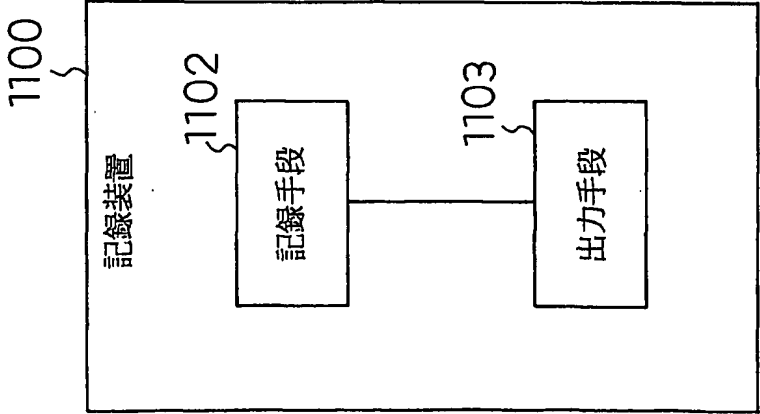
第30図



第32図



第31図

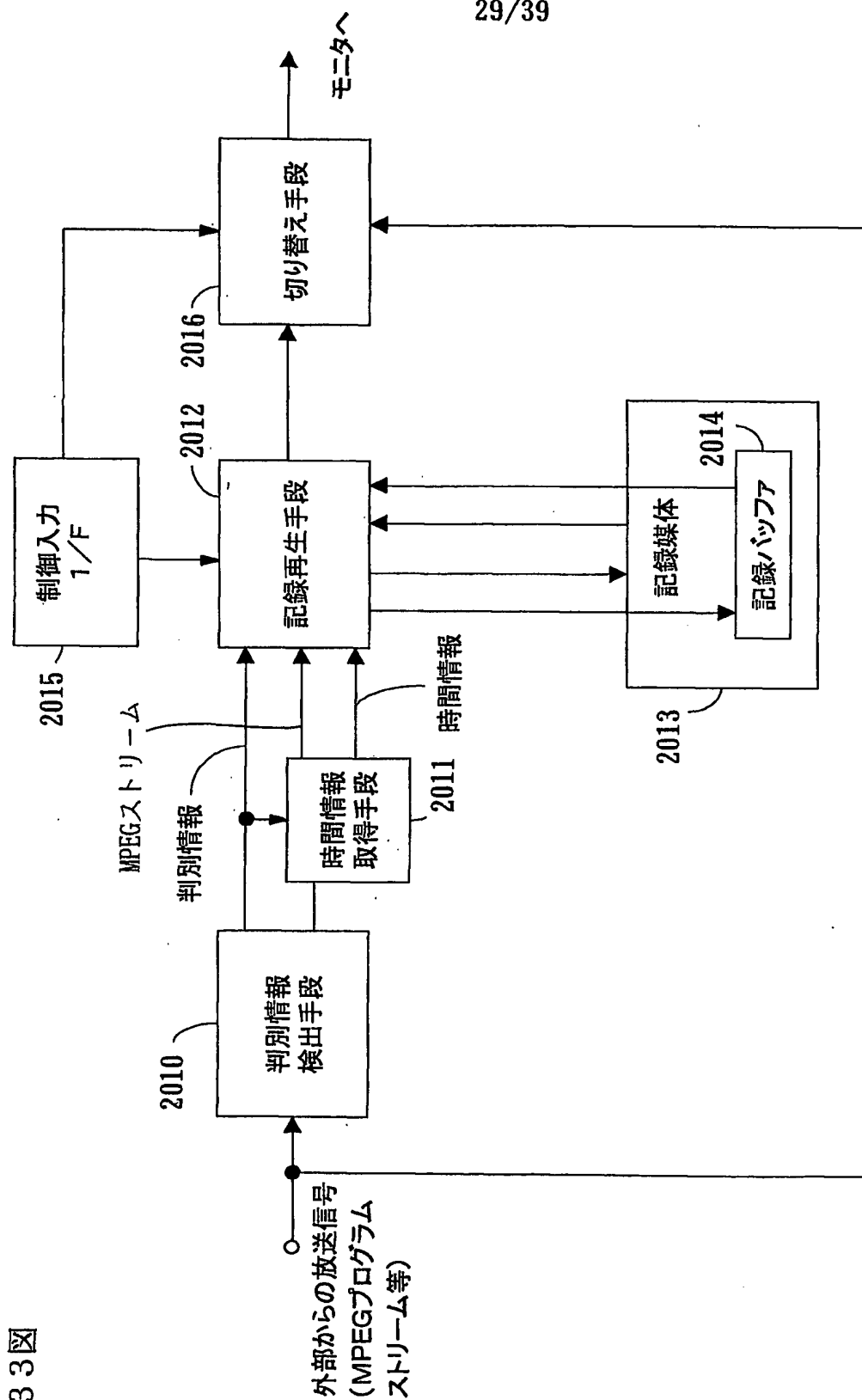


WO 01/48755

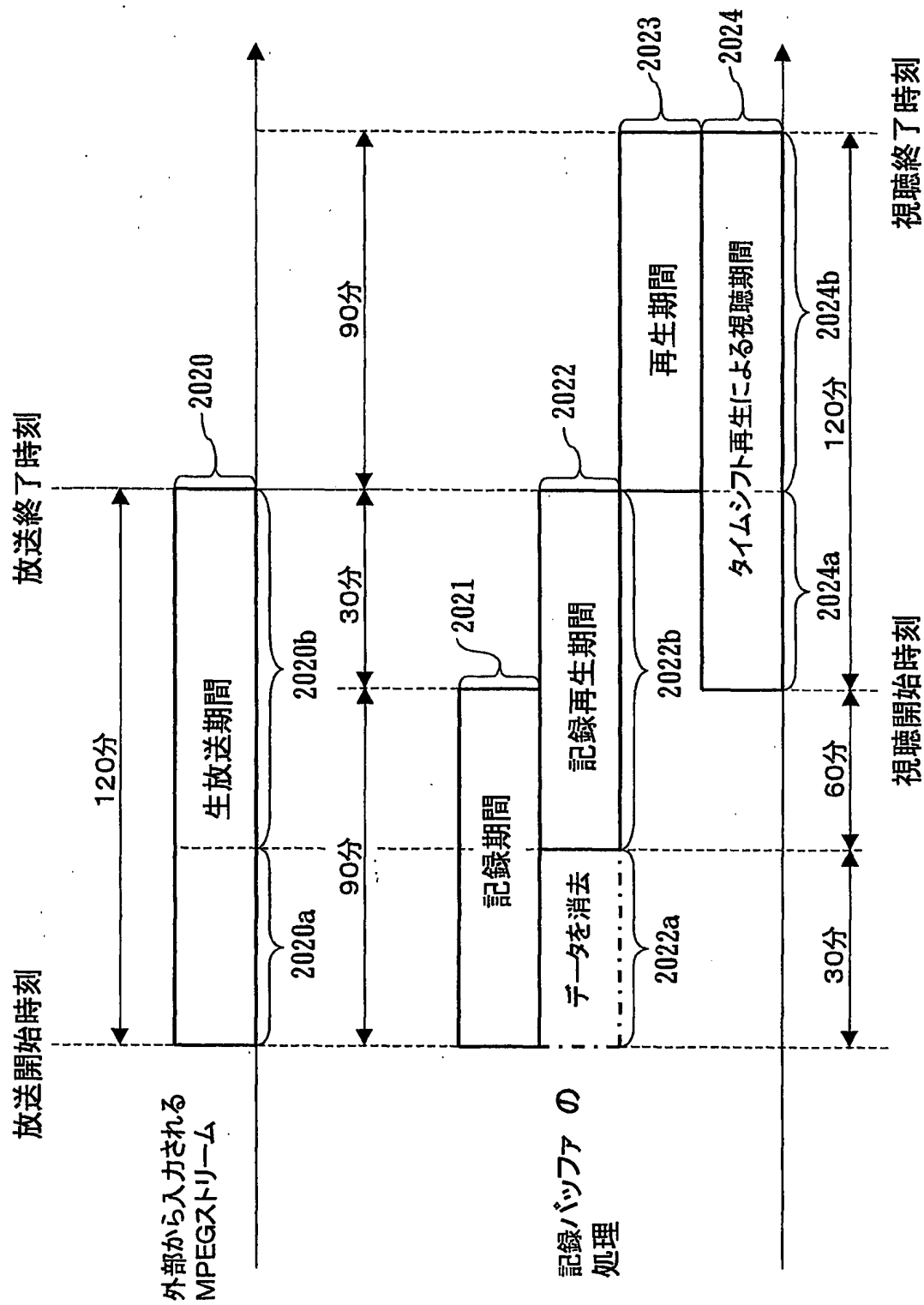
PCT/JP00/09260

29/39

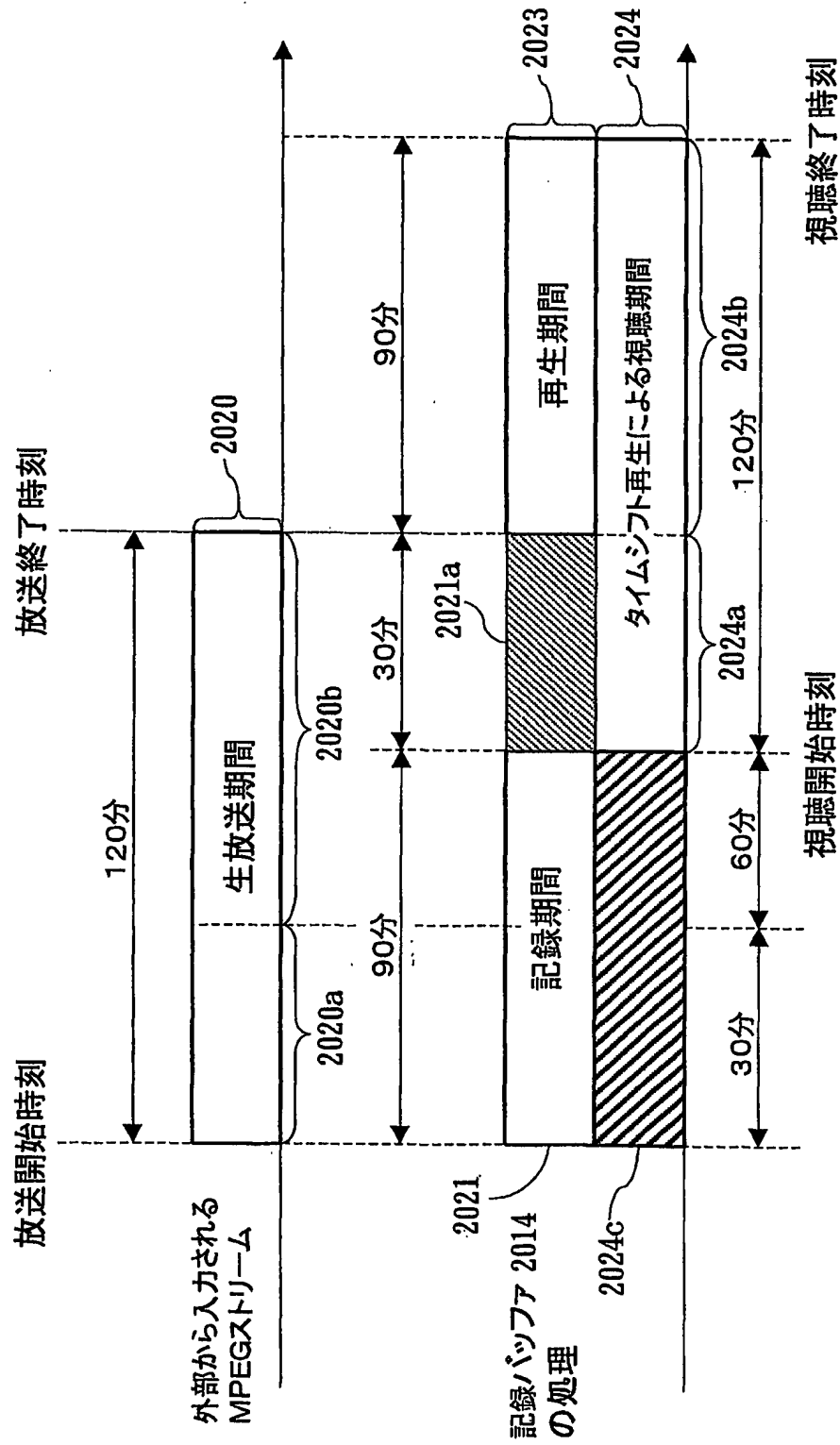
第33図



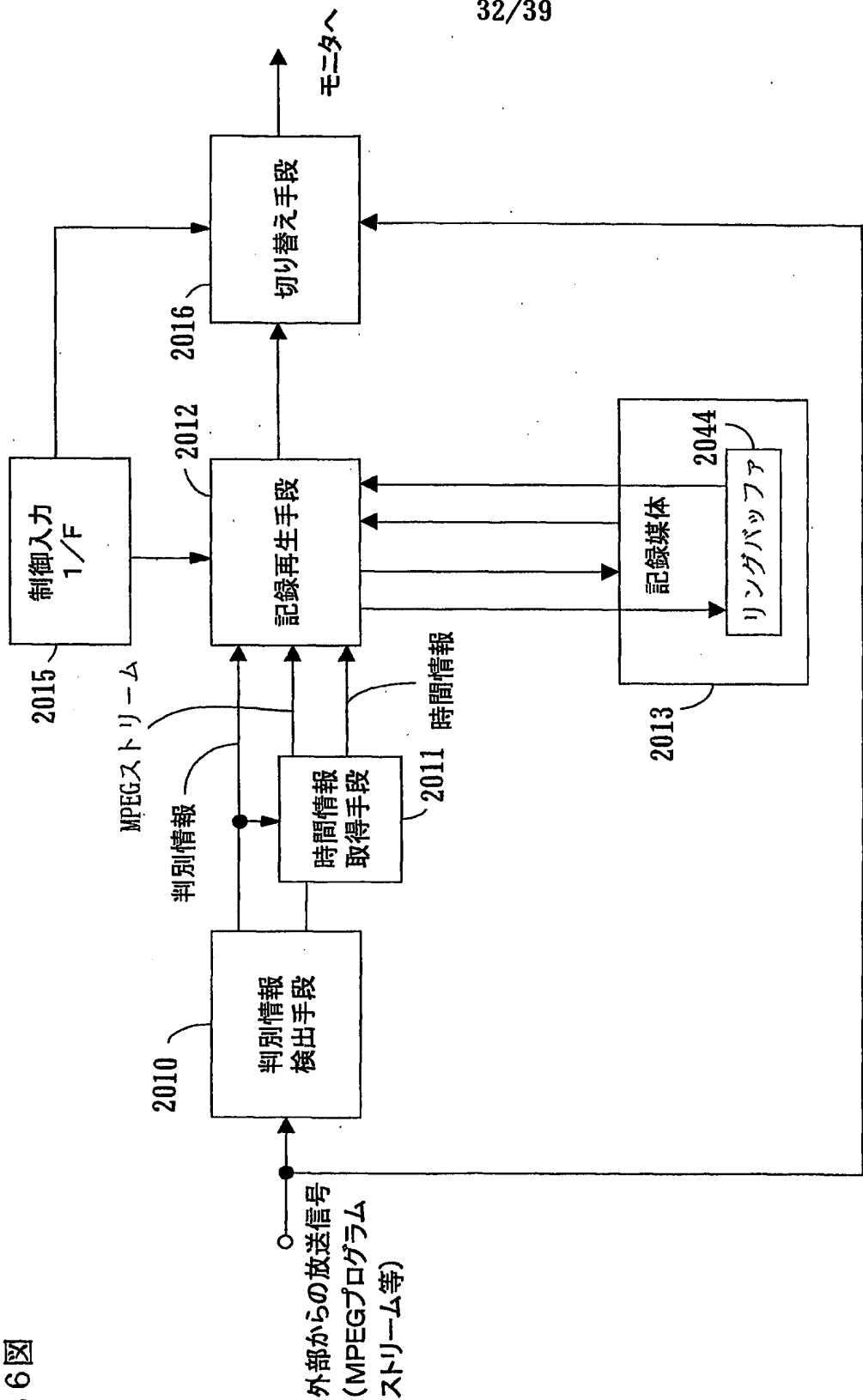
第34図



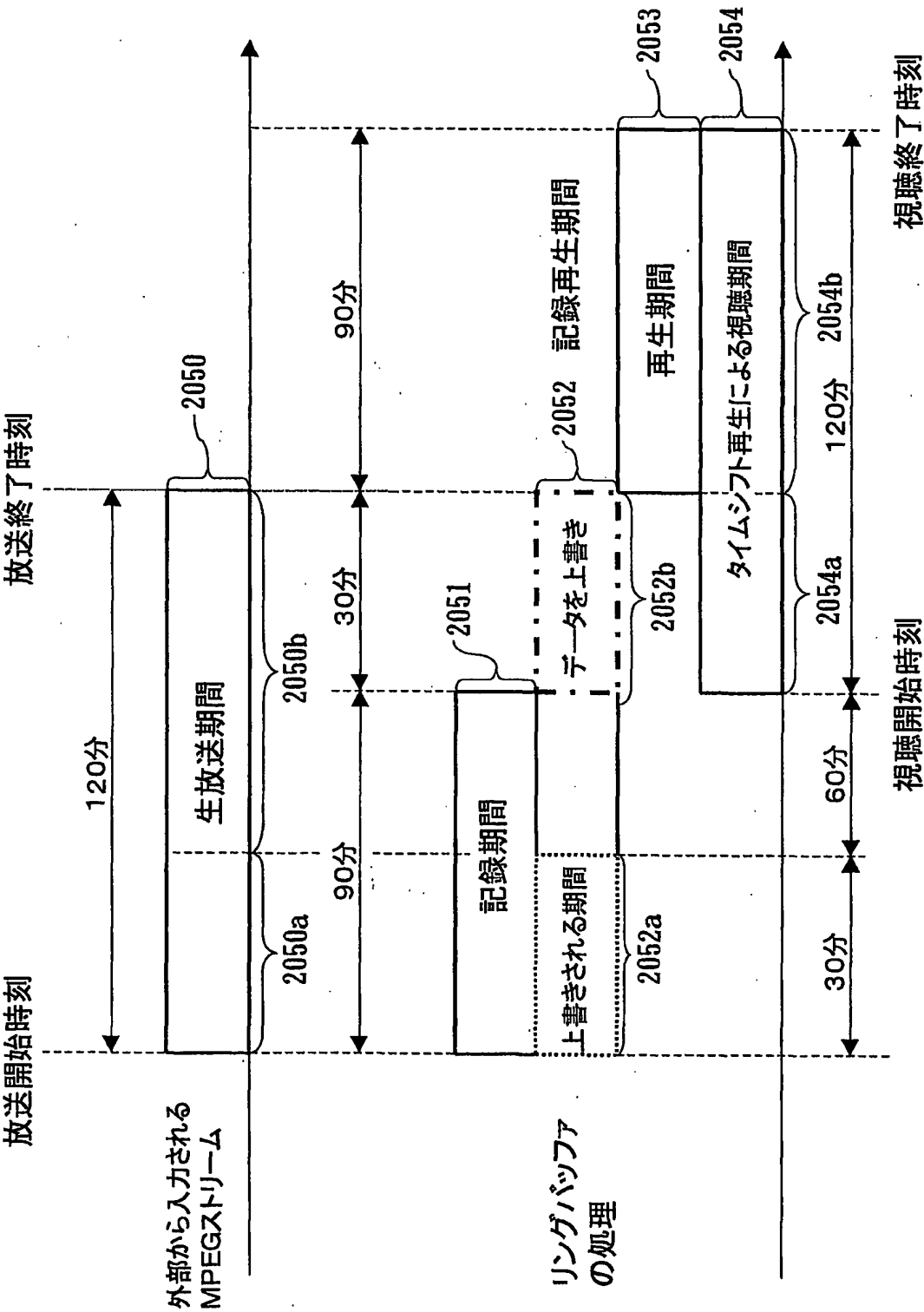
第35図



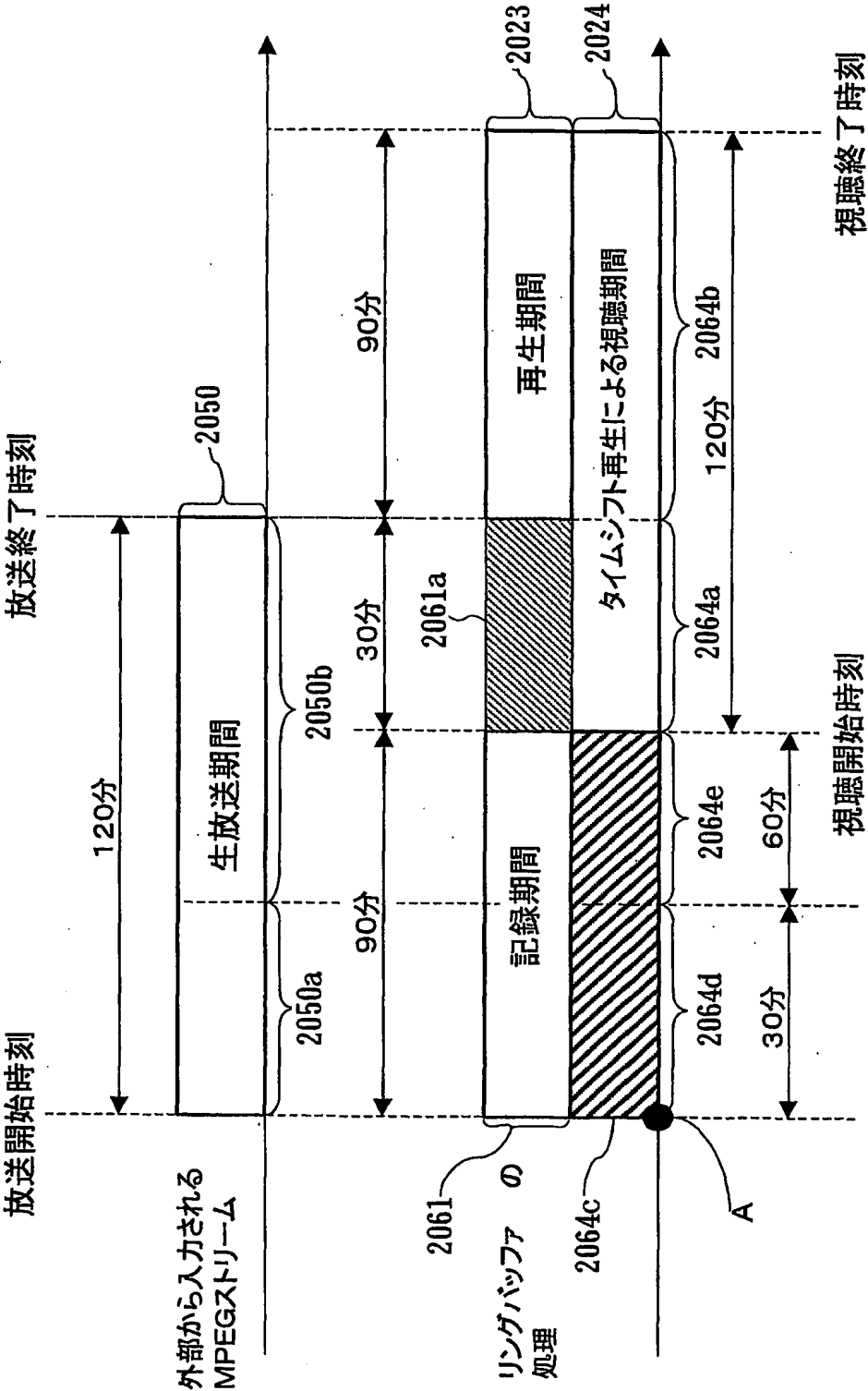
第36図



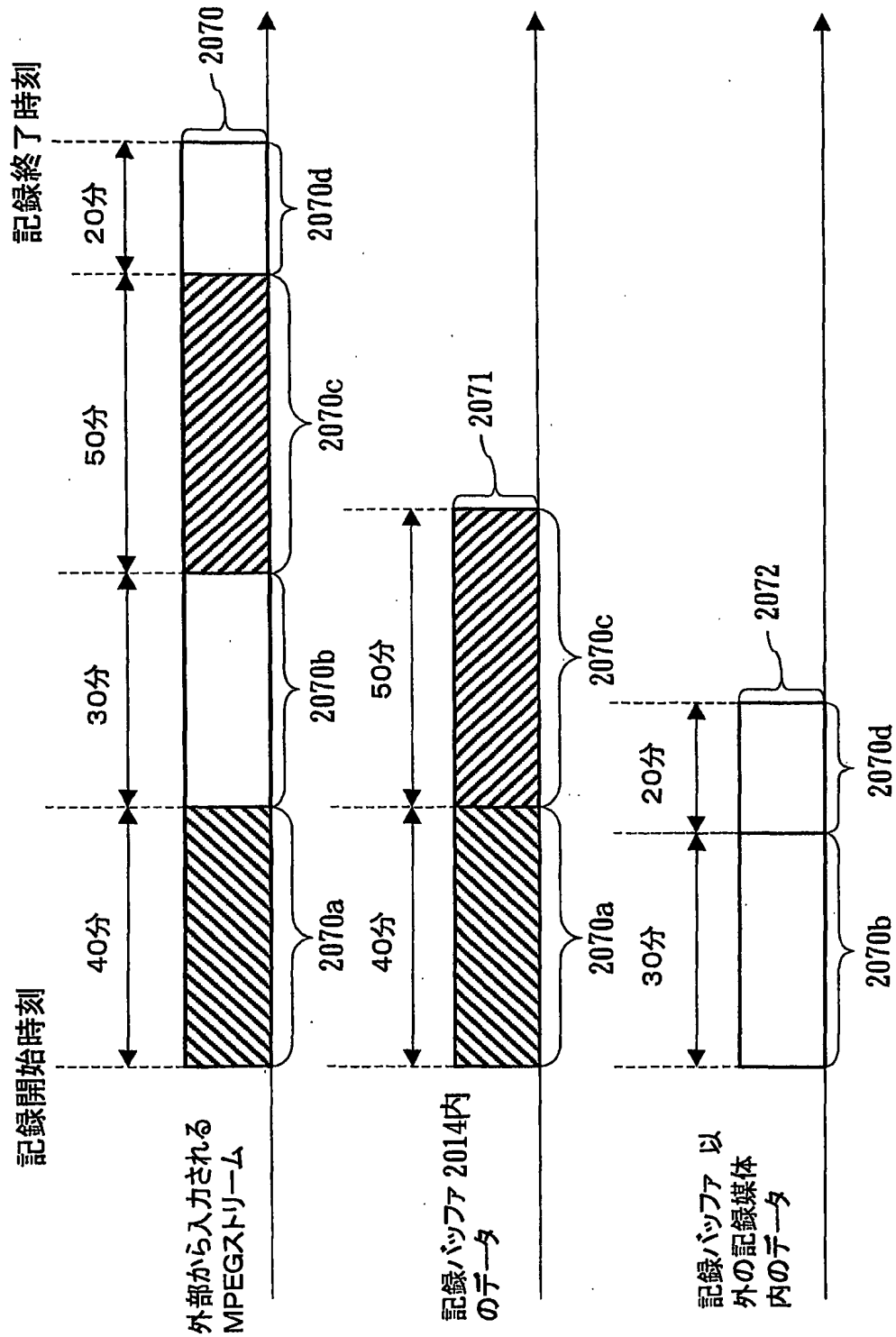
第37図



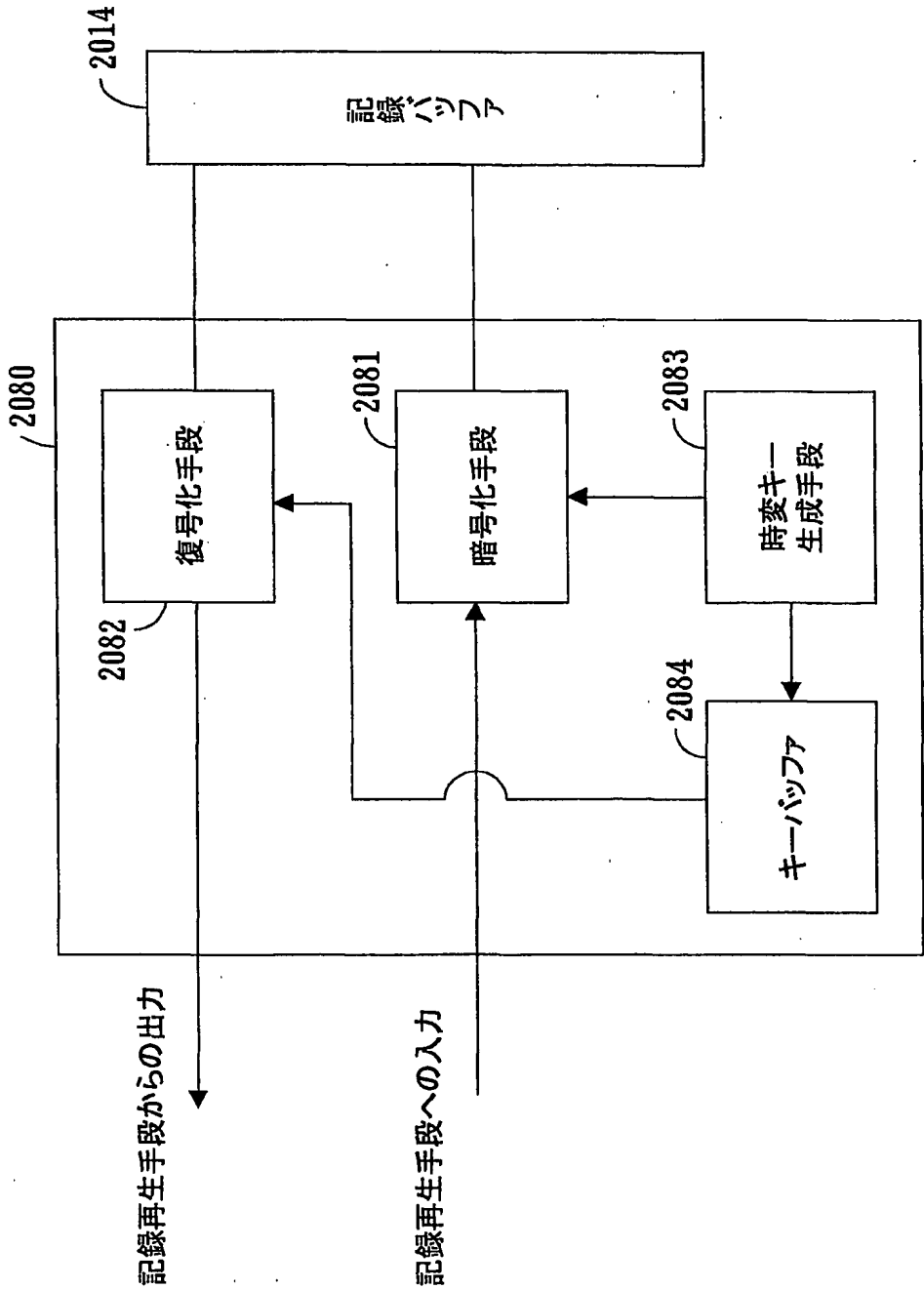
第38図



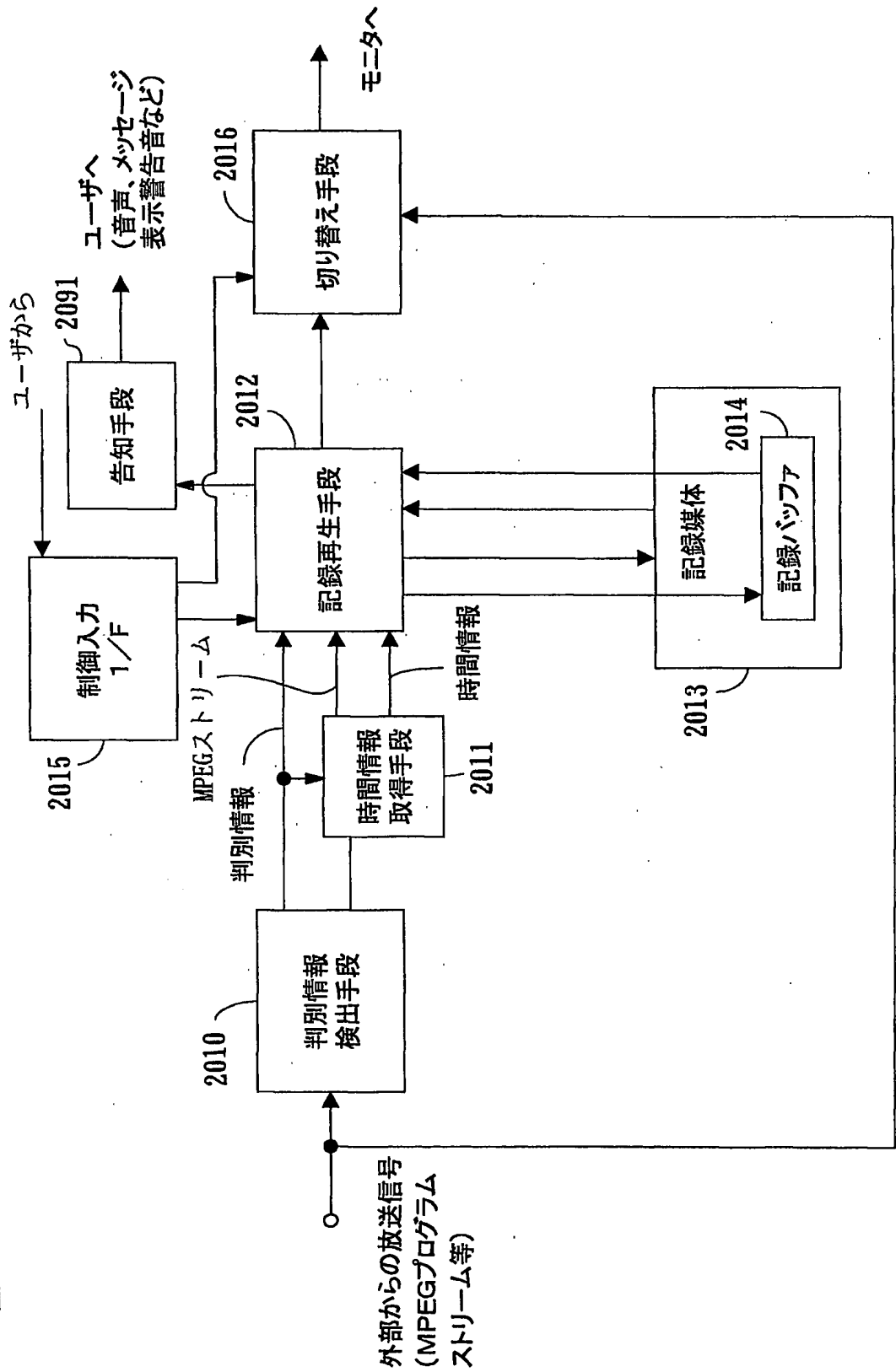
第39図



第40図

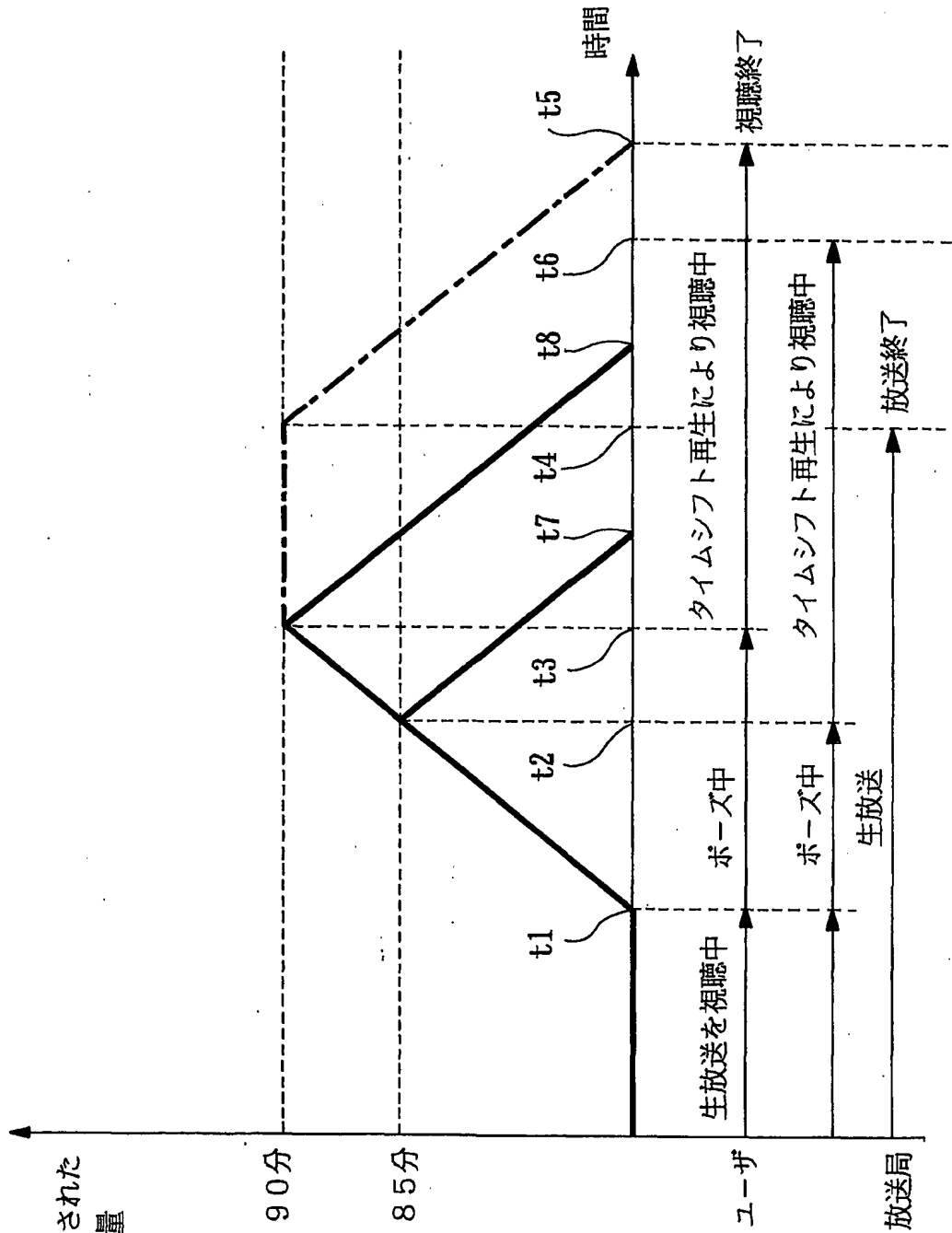


第41図

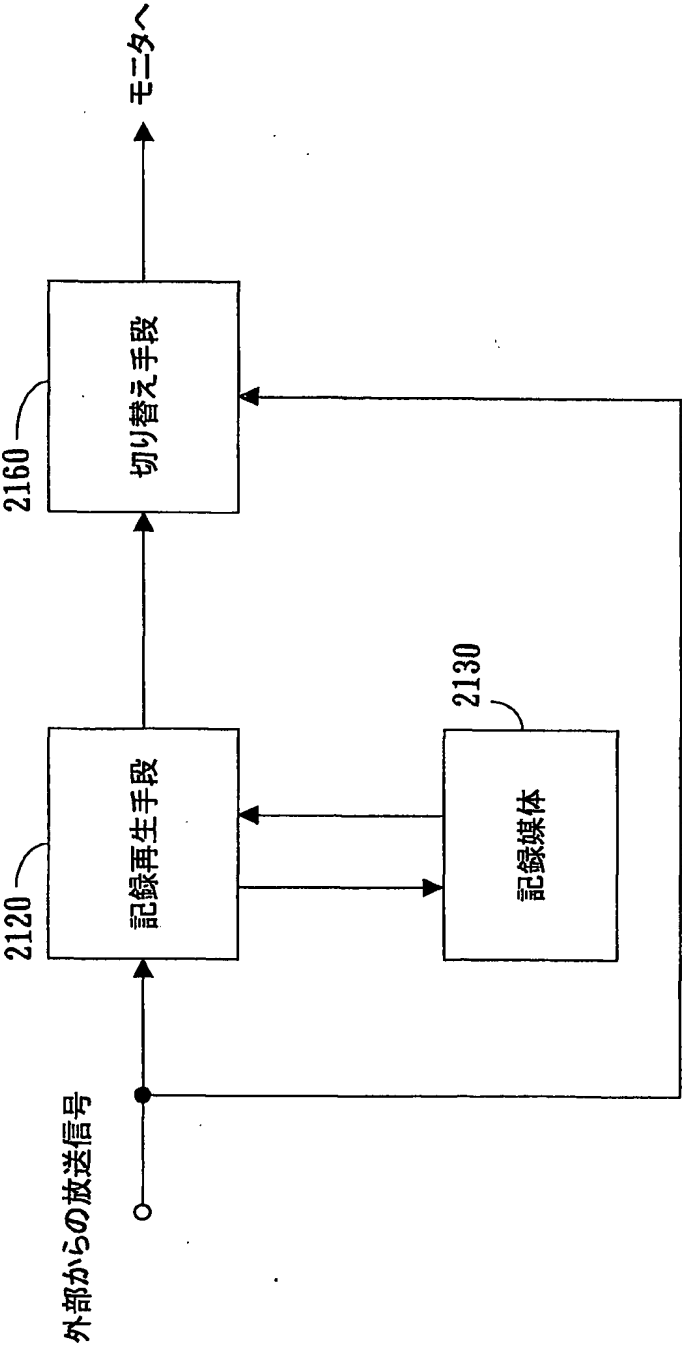


第42図

記録バッファに一時記録された
複製禁止コンテンツの残量



第43図



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/09260

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ G11B 20/10, G11B 20/12, G06F 17/60, G06F 3/06, H04N 5/91, H04L 9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ G11B 20/10, H04N 5/91

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 10-149619, A (Victor Company of Japan, Limited), 02 June, 1998 (02.06.98), Full text; Figs. 1 to 4 (Family: none)	1-74
Y A	JP, 10-40639, A (Sony Corporation), 13 February, 1998 (13.02.98), Full text; Figs. 1 to 5 (Family: none)	1-74 75
Y	JP, 11-86437, A (Toshiba Corporation), 30 March, 1999 (30.03.99), Full text; Figs. 1 to 8 (Family: none)	1-74
Y	JP, 9-191453, A (Sony Corporation), 22 July, 1997 (22.07.97), Full text; Figs. 1 to 16 & EP, 000740478, A2 & KR, 000231391, B & US, 006163644, A	76-95
Y	JP, 8-297919, A (Kabushiki Kaisha Hitachi Seisakusho Personal Media Kiki Jigyoubu), 12 July, 1996 (12.07.96), Full text; Figs. 1 to 10 (Family: none)	76-95

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 10 April, 2001 (10.04.01)	Date of mailing of the international search report 24 April, 2001 (24.04.01)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/09260

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 11-164254, A (Sony Electronics Inc.), 18 June, 1999 (18.06.99), Full text; Figs. 1 to 4 & NL, 001010109, A & GB, 002329997, A & DE, 019844635, A & GB, 009820939, A0	76-95
Y	JP, 10-56620, A (Matsushita Electric Ind. Co., Ltd.), 24 February, 1998 (24.02.98), Full text; Figs. 1 to 74 & EP, 000789488, A2 & CN, 001171012, A & US, 005999691, A1	85,86, 89,90

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/09260

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

See the extra sheet.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest ☐ The additional search fees were accompanied by the applicant's protest.
☒ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/09260

Continuation of Box No.II of continuation of first sheet (1)

The inventions of claims 1-21, 30-44 relate to an idea of recording copyright protection data on an HDD.

The inventions of claims 22-29 relate to an arrangement on a printed board.

The inventions of claims 45-75 relate to an idea of transferring/copying copyright protection data recorded on an HDD to another device.

The inventions of claims 76-95 relate to an idea of time-shift reproduction of copyright protection data recorded on an HDD.

国際調査報告		国際出願番号 PCT/J P 00/09260	
A. 発明の属する分野の分類 (国際特許分類 (IPC))			
Int. Cl ⁷ G11B 20/10、G11B 20/12、G06F 17/60、G06F 3/06、 H04N 5/91、H04L 9/00			
B. 調査を行った分野			
調査を行った最小限資料 (国際特許分類 (IPC))			
Int. Cl ⁷ G11B 20/10、H04N 5/91			
最小限資料以外の資料で調査を行った分野に含まれるもの			
日本国実用新案公報 1922-1996年 日本国公開実用新案公報 1971-2001年 日本国登録実用新案公報 1994-2001年 日本国実用新案登録公報 1996-2001年			
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)			
C. 関連すると認められる文献			
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号	
Y	J P, 10-149619, A (日本ビクター株式会社) 2. 6月. 1998 (02. 06. 98) 全文 第1-4図 (ファミリーなし)	1-74	
Y A	J P, 10-40639, A (ソニー株式会社) 13. 2月. 1998 (13. 02. 98) 全文 第1-5図 (ファミリーなし)	1-74 75	
<input checked="" type="checkbox"/> C欄の続きにも文献が列举されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。			
* 引用文献のカテゴリー			
「A」 特に関連のある文献ではなく、一般的技術水準を示すもの		「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの	
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの		「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの	
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)		「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの	
「O」 口頭による開示、使用、展示等に言及する文献		「&」 同一パテントファミリー文献	
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願			
国際調査を完了した日 10. 04. 01		国際調査報告の発送日 24.04.01	
国際調査機関の名称及びあて先 日本国特許庁 (ISA/J P) 郵便番号 100-8915 東京都千代田区霞が関三丁目4番3号		特許庁審査官 (権限のある職員) 宮下 誠 電話番号 03-3581-1101 内線 3589	

国際調査報告

国際出願番号 PCT/JPO0/09260

C (続き). 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	J P, 11-86437, A (株式会社東芝) 30. 3月. 1999 (30. 03. 99) 全文 第1-8図 (ファミリーなし)	1-74
Y	J P, 9-191453, A (ソニー株式会社) 22. 7月. 1997 (22. 07. 97) 全文 第1-16図 & E P, 000740478 , A 2 & K R, 000231391 , B & U S, 006163644 , A	76-95
Y	J P, 8-297919, A (株式会社日立製作所パーソナルメディア 機器事業部) 12. 7月. 1996 (12. 07. 96) 全文 第1-10図 (ファミリーなし)	76-95
Y	J P, 11-164254, A (ソニーエレクトロニクス インク) 18. 6月. 1999 (18. 06. 99) 全文 第1-4図 & N L, 001010109 , A & G B, 002329997 , A & D E, 019844635 , A & G B, 009820939 , A 0	76-95
Y	J P, 10-56620, A (松下電器産業株式会社) 24. 2月. 1998 (24. 02. 98) 全文 第1-74図 & E P, 000789488 , A 2 & C N, 001171012 , A & U S, 005999691 , A 1	85、86、 89、90

国際調査報告

国際出願番号 PCT/JPO0/09260

第I欄 請求の範囲の一部の調査ができないときの意見 (第1ページの2の続き)

法第8条第3項 (PCT 17条(2)(a)) の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. ☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 _____ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

第II欄 発明の単一性が欠如しているときの意見 (第1ページの3の続き)

次に述べるようにこの国際出願に二以上の発明があるところの国際調査機関は認めた。

発明の単一性が欠如している理由は特別ページに記載した。

1. ☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
- ☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

国際調査報告

国際出願番号 PCT/JP00/09260

請求の範囲1-21、30-44に係る発明は、HDDへの著作権保護データの記録に関するものである。

請求の範囲22-29に係る発明は、プリント基板上の配置に関するものである。

請求の範囲45-75に係る発明は、HDDに記録された著作権保護データの他の機器への移動・複製に関するものである。

請求の範囲76-95に係る発明は、HDDに記録された著作権保護データのタイムシフト再生に関するものである。